# Contents

## Introduction
- Revision history ........................................ 7
- Before you begin ........................................ 7
  - FortiGate models that support WAN optimization .......... 8
  - How this guide is organized .......................... 8

## Document conventions
- IP addresses ............................................ 9
- Cautions, Notes and Tips .............................. 9
- Typographical conventions ............................. 10
- CLI command syntax .................................. 11

## Registering your Fortinet product

## Fortinet products End User License Agreement

## Customer service and technical support

## Training

## Fortinet documentation
- Tools and Documentation CD ........................ 13
- Fortinet Knowledge Base ............................. 13
- Comments on Fortinet technical documentation ........ 13

## WAN optimization, web cache, and web proxy concepts
- WAN optimization topologies .......................... 15
  - Basic WAN optimization topologies .................. 16
  - Out-of-path topology ................................ 16
  - Topology for multiple networks .................... 17
  - Web-cache-only WAN optimization .................. 18
  - WAN optimization with web caching ................ 19
  - WAN optimization and web caching with FortiClient peers .......................... 20
- Web proxy topology .................................. 20
- WAN optimization client/server architecture ........ 21
  - WAN optimization peers ................................ 21
  - WAN optimization and the FortiClient application ........ 22
  - Operating modes and VDOMs .......................... 22
- WAN optimization tunnels ............................ 22
  - Tunnel sharing ....................................... 23
- Protocol optimization .................................. 24
| Contents |
|-----------------|--------|
| Byte caching     | 25     |
| WAN optimization and HA | 25     |
| Monitoring WAN optimization performance | 25 |
| WAN optimization, web cache and WCCP get and diagnose commands | 27 |
| **Peers and authentication groups** | 29 |
| Basic WAN optimization peer authentication requirements | 29 |
| Accepting any peers | 29 |
| How FortiGate units process tunnel requests for peer authentication | 30 |
| Configuring peers | 31 |
| Configuring authentication groups | 32 |
| Secure tunneling | 34 |
| **Configuring WAN optimization rules** | 37 |
| WAN optimization rules, firewall policies, and protection profiles | 37 |
| WAN optimization transparent mode | 38 |
| WAN optimization rule list | 38 |
| How list order affects rule matching | 40 |
| Moving a rule to a different position in the rule list | 41 |
| WAN optimization address formats | 42 |
| Configuring WAN optimization rules | 42 |
| Processing non-HTTP sessions accepted by an HTTP rule | 45 |
| Processing unknown HTTP sessions | 45 |
| **WAN optimization configuration examples** | 47 |
| Example: Basic active-passive WAN optimization | 47 |
| Network topology and assumptions | 47 |
| General configuration steps | 48 |
| Configuring basic active-passive WAN optimization - web-based manager | 48 |
| Configuring basic active-passive WAN optimization - CLI | 51 |
| Example: Basic peer-to-peer WAN optimization configuration | 53 |
| Network topology and assumptions | 54 |
| General configuration steps | 54 |
| Configuring basic peer-to-peer WAN optimization - web-based manager | 54 |
| Configuring basic peer-to-peer WAN optimization - CLI | 56 |
## SSL offloading for WAN optimization and web caching

- Example: SSL offloading for a WAN optimization tunnel .............................................. 103
  - Network topology and assumptions ........................................................................... 103
  - General configuration steps ...................................................................................... 104
  - Client-side configuration steps ................................................................................ 104
  - Server-side configuration steps ............................................................................... 106
- Example: SSL offloading and reverse proxy web caching for an Internet web server ............................................................................................................ 106
  - Network topology and assumptions ........................................................................... 107
  - Configuration steps .................................................................................................... 108

## FortiClient WAN optimization

- Configuring FortiClient WAN optimization ................................................................. 111
  - FortiClient configuration steps ................................................................................... 111
  - FortiGate unit configuration steps ............................................................................. 112

## The FortiGate explicit web proxy

- Applying protection profiles to explicit web proxy traffic ............................................ 113
- Configuring the explicit web proxy ............................................................................. 113
- Example: Explicit proxy configuration ....................................................................... 115
  - General configuration steps ...................................................................................... 115
  - Configuring the explicit web proxy - web-based manager .................................... 115
  - Configuring the explicit web proxy - CLI ................................................................. 116
- CLI configuration ......................................................................................................... 116
  - config web-proxy explicit ......................................................................................... 116
  - config web-proxy global ............................................................................................ 117

## WAN optimization storage

- Configuring WAN optimization storage ................................................................. 119
  - Syntax ......................................................................................................................... 119
  - Examples ..................................................................................................................... 120
- Example: WAN optimization storage on a FortiGate-111C unit with two hard disks ...................... 121
- About partition labels ................................................................................................. 122

## Index

- 123
Introduction

Welcome and thank you for selecting Fortinet products for your network protection.

You can use FortiGate WAN optimization and web caching to improve performance and security of traffic passing between locations on your wide area network (WAN) or from the Internet to your web servers. You can also use the FortiGate unit as an explicit web proxy server. If your FortiGate unit supports web caching, you can also add web caching to the web proxy server.

This document describes how FortiGate WAN optimization, web caching, and web proxy work and also describes how to configure these features.

This chapter contains the following topics:

- Revision history
- Revision history
- Document conventions
- Registering your Fortinet product
- Fortinet products End User License Agreement
- Customer service and technical support
- Training
- Fortinet documentation

Revision history

Table 1: Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-410-96996-20100127</td>
<td>Corrected subnet addresses in examples. In previous versions of this guide examples showed entering the address of a complete subnet as 172.20.120.0. The correct syntax for the web-based manager is 172.20.120.* and the correct syntax for the CLI is 172.20.120.0-172.20.120.255. Added “WAN optimization, web cache and WCCP get and diagnose commands” on page 27. Added “Applying protection profiles to explicit web proxy traffic” on page 113.</td>
</tr>
</tbody>
</table>

Before you begin

Before you begin using this guide, take a moment to note the following:

- Your FortiGate unit must support WAN optimization, web cache, and web proxy. See “FortiGate models that support WAN optimization” on page 8.

- If you enable virtual domains (VDOMs) on the FortiGate unit, WAN optimization, web caching, and web proxy are available separately for each VDOM. For details about configuring and using VDOMs, see the FortiGate VLAN and VDOM Guide.
• This guide is based on the assumption that you are a FortiGate administrator. It is not intended for others who may also use the FortiGate unit, such as FortiClient administrators or end users.

• Many configuration examples show steps for both the web-based manager (GUI) and the CLI. For more information about the commands and syntax used in this guide, see the following listings in the FortiGate CLI Reference:
  Under wanopt, see auth-group, cache-storage, peer, rule, settings, ssl-server, storage, and webcache,
  Under web-proxy, see explicit and global.

• FortiGate WAN optimization is proprietary to Fortinet. FortiGate WAN optimization is compatible only with FortiClient WAN optimization, and will not work with other vendors’ WAN optimization or acceleration features.

At this stage, the following installation and configuration conditions are assumed:
• You have already successfully installed two or more FortiGate units at various locations across your WAN by following the instructions in the appropriate FortiGate unit QuickStart or Installation Guide. You can download FortiGate installation guides from the FortiGate documentation page: http://docs.fortinet.com/fgt.html.
• You have administrative access to the web-based manager and/or CLI.
• The FortiGate units are integrated into your WAN.
• The operation mode has been configured.
• The system time, DNS settings, administrator password, and network interfaces have been configured.
• Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.
• You have added firewall policies to allow your FortiGate units to process traffic.

FortiGate models that support WAN optimization
WAN optimization is available on newer FortiGate models that also support SSL acceleration and byte caching and web caching storage locations such as high-capacity internal hard disks, the FortiGate-ASM-S08 AMC hard disk module, or FortiGate Storage Modules (FSMs). All of these storage locations can provide similar web caching and byte caching performance. If you add more than one storage location (for example, by creating multiple partitions on a storage device, by using more than one FSM, or by using and FSM and AMC hard disk in the same FortiGate unit) you can configure different storage locations for web caching and byte caching.
A storage location is only required for web caching and byte caching. All other WAN optimization features, including SSL acceleration, are supported if a storage location is not available.

You configure WAN optimization storage options from the FortiGate CLI. See “WAN optimization storage” on page 119.

How this guide is organized
This guide describes how to implement WAN optimization, web caching and the web proxy on supported FortiGate units.

The guide contains the following chapters:
WAN optimization, web cache, and web proxy concepts: Provides an overview of FortiGate WAN optimization best practices and technologies and some of the concepts and rules for using them. We recommend that you begin with this chapter before attempting to configure your FortiGate unit to use WAN optimization.
Peers and authentication groups: Describes how to use WAN optimization peers and authentication groups to control access to WAN optimization tunnels.

Configuring WAN optimization rules: Provides basic configuration for WAN optimization rules, including adding rules, organizing rules in the rule list and using WAN optimization addresses. This chapter also explains how WAN optimization accepts sessions, as well as how and when you can apply protection profiles to WAN optimization traffic.

WAN optimization configuration examples: Describes basic active-passive and peer-to-peer WAN optimization configuration examples. This chapter is a good place to start learning how to put an actual WAN optimization network together.

Web caching: Describes how WAN optimization web caching works to cache different session types, including HTTPS, and includes web caching configuration examples.

Advanced configuration example: Provides a configuration example that combines WAN optimization, web caching, out-of-path WAN optimization, and the use of multiple VDOMs to apply protection profiles to sessions being optimized.

SSL offloading for WAN optimization and web caching: Describes how to offload SSL processing from web sites to FortiGate units to improve WAN performance for SSL-protected web sites on a WAN.

FortiClient WAN optimization: Describes how FortiGate and FortiClient WAN optimization work together and includes an example configuration.

The FortiGate explicit web proxy: Describes the FortiGate web proxy and how to add web caching to a proxy configuration. This chapter includes guidance to pass to end-users when they need to configure their web browsers to use the proxy.

WAN optimization storage: Describes how to configure WAN optimization storage settings to control how data is stored for web caching and byte caching.

Document conventions

Fortinet technical documentation uses the conventions described below.

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at http://ietf.org/rfc/rfc1918.txt?number-1918.

Cautions, Notes and Tips

Fortinet technical documentation uses the following guidance and styles for cautions, notes and tips.

Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Note: Presents useful information, usually focused on an alternative, optional method, such as a shortcut, to perform a step.
**Tip:** Highlights useful additional information, often tailored to your workplace activity.

**Typographical conventions**

Fortinet documentation uses the following typographical conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button, menu, text box, field, or check box label</td>
<td>From <em>Minimum log level</em>, select <em>Notification</em>.</td>
</tr>
<tr>
<td>CLI input*</td>
<td>config system dns</td>
</tr>
<tr>
<td></td>
<td>set primary &lt;address_ipv4&gt;</td>
</tr>
<tr>
<td></td>
<td>end</td>
</tr>
<tr>
<td>CLI output</td>
<td>FGT-602803030703 # get system settings</td>
</tr>
<tr>
<td></td>
<td>comments : (null)</td>
</tr>
<tr>
<td></td>
<td>opmode : nat</td>
</tr>
<tr>
<td>Emphasis</td>
<td>HTTP connections are <strong>not</strong> secure and can be intercepted by a third party.</td>
</tr>
<tr>
<td>File content</td>
<td>&lt;HTML&gt;&lt;HEAD&gt;&lt;TITLE&gt;Firewall Authentication&lt;/TITLE&gt;&lt;/HEAD&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;BODY&gt;&lt;H4&gt;You must authenticate to use this service.&lt;/H4&gt;</td>
</tr>
<tr>
<td>Hyperlink</td>
<td>Visit the Fortinet Technical Support web site, <a href="https://support.fortinet.com">https://support.fortinet.com</a>.</td>
</tr>
<tr>
<td>Keyboard entry</td>
<td>Type a name for the remote VPN peer or client, such as Central_Office_1</td>
</tr>
<tr>
<td>Navigation</td>
<td>Go to <em>VPN &gt; IPSEC &gt; Auto Key (IKE)</em>.</td>
</tr>
<tr>
<td>Publication</td>
<td>For details, see the <a href="https://support.fortinet.com">FortiGate Administration Guide</a>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Links typically go to the most recent version. To access earlier releases, go to <a href="http://docs.fortinet.com/">http://docs.fortinet.com/</a>. This link appears at the bottom of each page of this document.</td>
</tr>
</tbody>
</table>

* For conventions used to represent command syntax, see “CLI command syntax” on page 11.
### CLI command syntax

This guide uses the following conventions to describe syntax to use when entering commands in the Command Line Interface (CLI).

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

For more information, see the *FortiGate CLI Reference*.

#### Table 3: Command syntax

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Square brackets** [ ] | A non-required word or series of words. For example: 
  
  ```
  [verbose {1 | 2 | 3}]
  ```
  
  indicates that you may either omit or type both the `verbose` word and its accompanying option, such as: 
  
  ```
  verbose 3
  ```

| **Angle brackets** < > | A word constrained by data type. 
  
  To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (\_) and suffix that indicates the valid data type. For example: 
  
  ```
  <retries_int>
  ```
  
  indicates that you should enter a number of retries, such as 5. 
  
  Data types include: 
  
  - `<xxx_name>`: A name referring to another part of the configuration, such as `policy_A`.
  - `<xxx_index>`: An index number referring to another part of the configuration, such as 0 for the first static route.
  - `<xxx_pattern>`: A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all email addresses ending in `@example.com`.
  - `<xxx_fqdn>`: A fully qualified domain name (FQDN), such as `mail.example.com`.
  - `<xxx_email>`: An email address, such as `admin@mail.example.com`.
  - `<xxx_ipv4>`: An IPv4 address, such as `192.168.1.99`.
  - `<xxx_ipv4range>`: An IPv4 address range.
  - `<xxx_v4mask>`: A dotted decimal IPv4 netmask, such as `255.255.255.0`.
  - `<xxx_ipv4mask>`: A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`.
  - `<xxx_ipv4/mask>`: A dotted decimal IPv4 address and CIDR notation netmask separated by a slash, such as `192.168.1.99/24`.
  - `<xxx_ipv6>`: An IPv6 address.
  - `<xxx_v6mask>`: A dotted decimal IPv6 netmask.
  - `<xxx_ipv6mask>`: A dotted decimal IPv6 address and netmask separated by a space.
  - `<xxx_str>`: A string of characters that is *not* another data type, such as `P@ssw0rd`. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences.
  - `<xxx_int>`: An integer number that is *not* another data type, such as 15 for the number of minutes.

| **Curly braces** { } | A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. 
  
  You must enter at least one of the options, unless the set of options is surrounded by square brackets [].

---

*FortiOS™ Handbook 4.0 MR1 FortiGate WAN Optimization, Web Cache and Web Proxy*  
*01-410-96996-20100127*  
*http://docs.fortinet.com/ • Feedback*
Registering your Fortinet product

Before you begin configuring and customizing features, take a moment to register your Fortinet product at the Fortinet Technical Support web site, https://support.fortinet.com. Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration. For more information, see the Fortinet Knowledge Base article Registration Frequently Asked Questions.

Fortinet products End User License Agreement

See the Fortinet products End User License Agreement.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that you can install your Fortinet products quickly, configure them easily, and operate them reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at https://support.fortinet.com.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Base article What does Fortinet Technical Support require in order to best assist the customer?

Training

Fortinet Training Services provides a variety of training programs to serve the needs of our customers and partners world-wide. Visit the Fortinet Training Services web site at http://campus.training.fortinet.com, or email training@fortinet.com.

Table 3: Command syntax

<table>
<thead>
<tr>
<th>Options delimited by vertical bars</th>
<th>Mutually exclusive options. For example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>{enable</td>
<td>disable}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Options delimited by spaces</th>
<th>Non-mutually exclusive options. For example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>{http https ping snmp ssh telnet}</td>
<td>indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: ping https ssh</td>
</tr>
<tr>
<td>Note: To change the options, you must re-type the entire list. For example, to add snmp to the previous example, you would type: ping https snmp ssh</td>
<td></td>
</tr>
<tr>
<td>If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.</td>
<td></td>
</tr>
</tbody>
</table>
Fortinet documentation

The Fortinet Technical Documentation web site, http://docs.fortinet.com, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Base.

Tools and Documentation CD

The documentation for your product is available on the Fortinet Tools and Documentation CD shipped with your product. The documents on this CD are current at shipping time. For the most current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, http://docs.fortinet.com.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com
WAN optimization, web cache, and web proxy concepts

FortiGate WAN optimization consists of a number of techniques that you can apply to improve the efficiency of communication across your WAN. These techniques include protocol optimization, byte caching, web caching, SSL offloading, and secure tunnelling. Protocol optimization can improve the efficiency of traffic that uses the CIFS, FTP, HTTP, or MAPI protocol, as well as general TCP traffic. Byte caching caches files and other data on FortiGate units to reduce the amount of data transmitted across the WAN. Web caching stores web pages on FortiGate units to reduce latency and delays between the WAN and web servers. SSL offloading offloads SSL decryption and encryption from web servers onto FortiGate SSL acceleration hardware. Secure tunnelling secures traffic as it crosses the WAN.

You can apply different combinations of these WAN optimization techniques to a single traffic stream depending on the traffic type. For example, you can apply byte caching and secure tunneling to any TCP traffic. For HTTP traffic, you can also apply protocol optimization and web caching.

Web proxy is a feature related to WAN optimization and web caching. You can configure a FortiGate unit to be a web proxy server. Users on your internal network can browse the Internet through the FortiGate web proxy server. If your FortiGate unit supports web caching, you can add web caching to the web proxy.

This chapter describes:
- WAN optimization topologies
- Web proxy topology
- WAN optimization client/server architecture
- WAN optimization tunnels
- Protocol optimization
- Byte caching
- WAN optimization and HA
- Monitoring WAN optimization performance
- WAN optimization, web cache and WCCP get and diagnose commands

WAN optimization topologies

This section describes some common WAN optimization topologies:
- “Basic WAN optimization topologies” on page 16
- “Out-of-path topology” on page 16
- “Web-cache-only WAN optimization” on page 18
- “WAN optimization with web caching” on page 19
- “WAN optimization and web caching with FortiClient peers” on page 20
**Basic WAN optimization topologies**

The basic FortiGate WAN optimization topology consists of two FortiGate units operating as WAN optimization peers intercepting and optimizing traffic crossing the WAN between the private networks.

**Figure 1: Security device and WAN optimization topology**

As shown in Figure 1, the FortiGate units can be deployed as security devices that protect private networks connected to the WAN and also perform WAN optimization. In this configuration, the FortiGate units are configured as typical security devices for the private networks and are also configured for WAN optimization. The WAN optimization configuration intercepts traffic to be optimized as it passes through the FortiGate unit and uses a WAN optimization tunnel with another FortiGate unit to optimize the traffic that crosses the WAN.

As shown in Figure 2, you can also deploy WAN optimization on single-purpose FortiGate units that only perform WAN optimization. In Figure 2, the WAN optimization FortiGate units are located on the WAN outside of the private networks. You can also install the WAN optimization FortiGate units behind the security devices on the private networks.

**Figure 2: Single-purpose WAN optimization topology**

The WAN optimization configuration is the same for FortiGate units deployed as security devices and for single-purpose WAN optimization FortiGate units. The only differences would result from the different network topologies.

**Out-of-path topology**

In an out-of-path topology, one or both of the FortiGate units configured for WAN optimization are not directly in the main data path. Instead, the out-of-path FortiGate unit is connected to a device on the data path, and the device is configured to redirect sessions to be optimized to the out-of-path FortiGate unit.
Figure 3 shows out-of-path FortiGate units configured for WAN optimization and connected directly to FortiGate units in the data path. The FortiGate units in the data path use a method such as policy routing to redirect traffic to be optimized to the out-of-path FortiGate units. The out-of-path FortiGate units establish a WAN optimization tunnel between each other and optimize the redirected traffic.

**Figure 3: Out-of-path WAN optimization**

One of the benefits of out-of-path WAN optimization is that out-of-path FortiGate units only perform WAN optimization and do not have to process other traffic. An in-path FortiGate unit configured for WAN optimization also has to process other non-optimized traffic on the data path.

The out-of-path FortiGate units can operate in NAT/Route or Transparent mode.

Other out-of-path topologies are also possible. For example, you can install the out-of-path FortiGate units on the private networks instead of on the WAN. Also, the out-of-path FortiGate units can have one connection to the network instead of two. In a one-arm configuration such as this, firewall policies and routing have to be configured to send the WAN optimization tunnel out the same interface as the one that received the traffic.

**Topology for multiple networks**

As shown in Figure 4, you can create multiple WAN optimization configurations between many private networks. Whenever WAN optimization occurs, it is always between two FortiGate units, but you can configure any FortiGate unit to perform WAN optimization with any of the other FortiGate units that are part of your WAN.
You can also configure WAN optimization between FortiGate units with different roles on the WAN. FortiGate units configured as security devices and for WAN optimization can perform WAN optimization as if they are single-purpose FortiGate units just configured for WAN optimization.

**Web-cache-only WAN optimization**

A WAN optimization web-cache-only topology includes one FortiGate unit that acts as both a proxy server and web cache server. The FortiGate unit intercepts web page requests sent by users, requests web pages from the web servers, caches the web page contents, and returns the web page contents to the users. When the FortiGate unit intercepts subsequent requests for cached web pages, the FortiGate unit contacts the destination web server just to check for changes.
WAN optimization, web cache, and web proxy concepts

WAN optimization topologies

Figure 5: Web-cache-only topology

You can also configure a reverse proxy web-cache-only WAN optimization (Figure 6). In this configuration, users on the Internet browse to a web server installed behind a FortiGate unit. The FortiGate unit intercepts the web traffic and caches pages from the web server. Reverse proxy web caching on the FortiGate unit reduces the number of requests that the web server must handle, leaving it free to process new requests that it has not serviced before.

Figure 6: Reverse proxy web caching

WAN optimization with web caching

You can add web caching to a WAN optimization topology when users on a private network communicate with web servers located across the WAN on another private network.

Figure 7: WAN optimization with web caching topology

The topology in Figure 7 is the same as that of Figure 1 on page 16 with the addition of web caching to the FortiGate unit in front of the private network that includes the web servers. In a similar way, you can add web caching to all of the topologies shown in "WAN optimization topologies" on page 15.
WAN optimization and web caching with FortiClient peers

FortiClient WAN optimization works with FortiGate WAN optimization to accelerate remote user access to the private networks behind FortiGate units. The FortiClient application requires a simple WAN optimization configuration to automatically detect if WAN optimization is enabled on the FortiGate unit. Once WAN optimization is enabled, the FortiClient application transparently makes use of the WAN optimization and web caching features available.

Figure 8: FortiClient WAN optimization topology

Web proxy topology

You can use the FortiGate web proxy to configure a FortiGate unit to be an explicit web proxy server for Internet web browsing. When configuring their web browser proxy, users must add the IP address of the FortiGate unit interface that they connect to.

Figure 9: Explicit web proxy topology

If your FortiGate unit supports web caching, you can also add web caching to the explicit web proxy. The FortiGate unit will then caches Internet web pages to improve web browsing performance.
WAN optimization client/server architecture

Traffic across a WAN typically consists of clients on a client network communicating across a WAN with a remote server network. The clients do this by starting communication sessions from the client network to the server network. To optimize these sessions, you add firewall policies to the client-side FortiGate unit (which is located between the client network and the WAN, see Figure 11) to accept sessions from the client network that are destined for the server network. To apply WAN optimization to these sessions, you must also add WAN optimization rules to the client-side FortiGate unit. The WAN optimization rules intercept sessions accepted by firewall policies and apply WAN optimization to them.

When a client-side FortiGate unit matches a session with a WAN optimization rule, it uses the information in the rule to attempt to start a WAN optimization tunnel with a server-side FortiGate unit installed in front of the server network. This FortiGate unit must include a WAN optimization rule to accept WAN optimization tunnel requests from the client-side FortiGate unit.

Firewall policies are not required on the server-side FortiGate unit. Sessions from the client-side to the server-side FortiGate unit are WAN optimization tunnel requests. As long as the server-side FortiGate unit contains WAN optimization rules, it will accept WAN optimization tunnel requests. These tunnel requests, however, will only result in an operating tunnel if the FortiGate unit peers can authenticate with each other.

WAN optimization peers

The client-side and server-side FortiGate units are called WAN optimization peers (see Figure 12) because all of the FortiGate units in a WAN optimization network have the same peer relationship with each other. The client and server roles just relate to how a session is started. Any FortiGate unit configured for WAN optimization can be a client-side and a server-side FortiGate unit at the same time, depending on the direction of the traffic. Client-side FortiGate units initiate WAN optimization sessions and server-side FortiGate units respond to the session requests. Any FortiGate unit can simultaneously be a client-side FortiGate unit for some sessions and a server-side FortiGate unit for others.
To identify all of the WAN optimization peers that a FortiGate unit can perform WAN optimization with, you add host IDs and IP addresses of all of the peers to the FortiGate unit configuration. The peer IP address is actually the IP address of the peer unit interface that communicates with the FortiGate unit.

**WAN optimization and the FortiClient application**

PCs running the FortiClient application are client-side peers that initiate WAN optimization tunnels with server-side peer FortiGate units. However, you can have an ever-changing number of FortiClient peers with IP addresses that also change regularly. To avoid maintaining a list of such peers, you can instead configure WAN optimization to accept any peer and use authentication to identify FortiClient peers.

Together, the WAN optimization peers apply the WAN optimization features to optimize the traffic flow over the WAN between the clients and servers. WAN optimization reduces bandwidth requirements, increases throughput, reduces latency, offloads SSL encryption/decryption and improves privacy for traffic on the WAN.

**Operating modes and VDOMs**

To use WAN optimization, the FortiGate units can operate in either NAT/Route or Transparent mode. The client-side and server-side FortiGate units do not have to be operating in the same mode.

As well, the FortiGate units can be configured for multiple virtual domain (VDOM) operation. You configure WAN optimization for each VDOM and configure one or both of the units to operate with multiple VDOMs enabled.

If a FortiGate unit or VDOM is operating in Transparent mode with WAN optimization enabled, WAN optimization uses the management IP address as the peer IP address of the FortiGate unit instead of the address of an interface.

**WAN optimization tunnels**

All optimized traffic passes between the FortiGate units or between a FortiClient peer and a FortiGate unit over a WAN optimization tunnel. Traffic in the tunnel can be sent in plain text or encrypted using AES-128bit-CBC SSL. Both the plain text and the encrypted tunnels use TCP port 7810.
Before a tunnel can be started, the peers must be configured to authenticate with each other and to agree on the tunnel configuration. Then, the client-side peer attempts to start a WAN optimization tunnel with the server-side peer. Once the peers authenticate with each other, they bring up the tunnel and WAN optimization communication over the tunnel starts. After a tunnel has been established, multiple WAN optimization sessions can start and stop between peers without restarting the tunnel.

**Tunnel sharing**

You can use the `tunnel-sharing` WAN optimization rule CLI keyword to configure tunnel sharing for WAN optimization rules with `auto-detect` set to `off`. Tunnel sharing means multiple WAN optimization sessions share the same WAN optimization tunnel. Tunnel sharing can improve WAN performance by reducing the number of WAN optimization tunnels between FortiGate units. Having fewer tunnels means less data to manage. Also, tunnel setup requires more than one exchange of information between the ends of the tunnel. Once the tunnel is set up, each new session that shares the tunnel avoids tunnel setup delays.

Tunnel sharing also uses bandwidth more efficiently by reducing the chances that small packets will be sent down the tunnel. Processing small packets reduces network throughput, so reducing the number of small packets improves performance. A shared tunnel can combine all the data from the sessions being processed by the tunnel and send the data together. For example, suppose a FortiGate unit is processing five WAN optimization sessions and each session has 100 bytes to send. If these sessions use a shared tunnel, WAN optimization combines the packets from all five sessions into one 500-byte packet. If each session uses its own private tunnel, five 100-byte packets will be sent instead. Each packet also requires a TCP ACK reply. The combined packet in the shared tunnel requires one TCP ACK packet. The separate packets in the private tunnels require five.

Tunnel sharing is not always recommended. Aggressive and non-aggressive protocols should not share the same tunnel. An aggressive protocol can be defined as a protocol that is able to get more bandwidth than a non-aggressive protocol. (The aggressive protocols can “starve” the non-aggressive protocols.) HTTP and FTP are considered aggressive protocols. If aggressive and non-aggressive protocols share the same tunnel, the aggressive protocols may take all of the available bandwidth. As a result, the performance of less aggressive protocols could be reduced. To avoid this problem, rules for HTTP and FTP traffic should have their own tunnel. To do this, set `tunnel-sharing` to `private` for WAN optimization rules that accept HTTP or FTP traffic.
It is also useful to set tunnel-sharing to express-sharing for applications, such as Telnet, that are very interactive but not aggressive. Express sharing optimizes tunnel sharing for Telnet and other interactive applications where latency or delays would seriously affect the user’s experience with the protocol.

Set tunnel-sharing to sharing for applications that are not aggressive and are not sensitive to latency or delays. WAN optimization rules set to sharing and express-sharing can share the same tunnel.

Protocol optimization

Protocol optimization techniques optimize bandwidth use across the WAN. These techniques can improve the efficiency of communication across the WAN optimization tunnel by reducing the amount of traffic required by communication protocols. You can apply protocol optimization to Common Internet File System (CIFS), FTP, HTTP, MAPI, and general TCP sessions.

For example, CIFS provides file access, record locking, read/write privileges, change notification, server name resolution, request batching, and server authentication. CIFS is a fairly “chatty” protocol, requiring many background transactions to successfully transfer a single file. This is usually not a problem across a LAN. However, across a WAN, latency and bandwidth reduction can slow down CIFS performance.

When you set Protocol to CIFS in a WAN optimization rule, the FortiGate units at both ends of the WAN optimization tunnel use a number of techniques to reduce the number of background transactions that occur over the WAN for CIFS traffic.

You can select only one protocol in a WAN optimization rule. For best performance, you should separate the traffic by protocol by creating different WAN optimization rules for each protocol. For example, to optimize HTTP traffic, you should set Port to 80 so that only HTTP traffic is accepted by this WAN optimization rule. For an example configuration that uses multiple rules for different protocols, see “Example: Basic active-passive WAN optimization” on page 47.

Figure 14: Example WAN optimization rule to optimize HTTP traffic

<table>
<thead>
<tr>
<th>New Wan Optimization Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node</strong></td>
</tr>
<tr>
<td><strong>Source</strong></td>
</tr>
<tr>
<td>172.20.150*</td>
</tr>
<tr>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td>192.168.10.*</td>
</tr>
<tr>
<td><strong>Port</strong></td>
</tr>
<tr>
<td>80</td>
</tr>
<tr>
<td><strong>Auto-Detect</strong></td>
</tr>
<tr>
<td>Active</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
</tr>
<tr>
<td>HTTP</td>
</tr>
<tr>
<td><strong>Transparent Mode</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Enable Byte Caching</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Enable SSL</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Enable Secure Tunnel</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Authentication Group</strong></td>
</tr>
<tr>
<td>(Please Select)</td>
</tr>
</tbody>
</table>

If the WAN optimization accepts a range of different types of traffic, you can set Protocol to TCP to apply general optimization techniques to TCP traffic. However, applying this TCP optimization to a range of different types of traffic is not as effective as applying more protocol-specific optimization to specific types of traffic. TCP protocol optimization uses techniques such as TCP SACK support, TCP window scaling and window size adjustment, and TCP connection pooling to remove TCP bottlenecks.
Byte caching

Byte caching breaks large units of application data (for example, a file being downloaded from a web page) into small chunks of data, labeling each chunk of data with a hash of the chunk and storing those chunks and their hashes in a database. The database is stored on a WAN optimization storage device. Then, instead of sending the actual data over the WAN tunnel, the FortiGate unit sends the hashes. The FortiGate unit at the other end of the tunnel receives the hashes and compares them with the hashes in its local byte caching database. If any hashes match, that data does not have to be transmitted over the WAN optimization tunnel. The data for any hashes that do not match is transferred over the tunnel and added to that byte caching database. Then the unit of application data (the file being downloaded) is reassembled and sent to its destination.

Byte caching is not application specific. Bytes cached from a file in an email can be used to optimize downloading that same file or a similar file from a web page. The result is less data transmitted over the WAN. Initially, byte caching may reduce performance until a large enough byte caching database is built up.

To enable byte caching, you select Enable Byte Cache in a WAN optimization rule. The Protocol setting does not affect byte caching. Data is byte cached when it is processed by a WAN optimization rule that includes byte caching.

Byte caching cannot determine whether or not a file is compressed (for example a zip file), and caches compressed and non-compressed versions of the same file separately.

WAN optimization and HA

You can configure WAN optimization on a FortiGate HA cluster. The recommended HA configuration for WAN optimization is active-passive mode. When the cluster is operating, all WAN optimization sessions are processed by the primary unit only. Even if the cluster is operating in active-active mode, HA does not load-balance WAN optimization sessions.

You can also form a WAN optimization tunnel between a cluster and a standalone FortiGate unit or between two clusters.

In a cluster, the primary unit stores only web cache and byte cache databases. These databases are not synchronized to the subordinate units. So, after a failover, the new primary unit must rebuild its web and byte caches.

Rebuilding the byte caches can happen relatively quickly because the new primary unit gets byte cache data from the other FortiGate units that it is participating with in WAN optimization tunnels.

Monitoring WAN optimization performance

Using WAN optimization monitoring, you can view and improve WAN optimization performance. The monitoring tools help isolate performance problems, aid in troubleshooting, and enable network optimization and capacity planning.

The monitor unit presents collected log information in a graphical format to show network traffic summary and bandwidth optimization information.

To view the WAN optimization monitor, go to WAN Opt. & Cache > Monitor.
This section provides traffic optimization information. The pie chart illustrates the percentage of traffic for supported applications processed during the selected Period. The table displays how much traffic has been reduced by WAN optimization by comparing the amount of LAN and WAN traffic for each protocol.

**Refresh icon**
Refresh the Traffic Summary.

**Period**
Select a time period to show traffic summary for. You can select:
- Last 10 Minutes
- Last 1 Hour
- Last 1 Day
- Last 1 Week
- Last 1 Month

**Protocol**
The name of the protocol for which sessions are optimized.

**Reduction Rate**
Displays each application’s optimization rate. For example, a rate of 80% means the amount of data processed by that application has been reduced by 20%.

**LAN**
The amount of data in MB received from the LAN for each application.

**WAN**
The amount of data in MB sent across the WAN for each application. The greater the difference between the LAN and WAN data, the greater the amount of data reduced by WAN optimization byte caching, web caching, and protocol optimization.

**Bandwidth Optimization**
This section shows network bandwidth optimization per time period. A line or column chart compares an application’s pre-optimized (LAN data) size with its optimized size (WAN data).
### WAN optimization, web cache and WCCP get and diagnose commands

The following diagnose and get commands are available for troubleshooting WAN optimization, web cache, and WCCP.

#### Table 4: WAN optimization, web cache, and WCCP get and diagnose commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>diagnose wad</code> {console-log</td>
<td>filter</td>
</tr>
<tr>
<td><code>diagnose wacs</code> {clear</td>
<td>recents</td>
</tr>
<tr>
<td><code>diagnose wadb</code> {check</td>
<td>clear</td>
</tr>
<tr>
<td><code>diagnose debug application</code> {wad</td>
<td>wa_cs</td>
</tr>
</tbody>
</table>
### Table 4: WAN optimization, web cache, and WCCP get and diagnose commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get test {wad</td>
<td>wa_cs</td>
</tr>
<tr>
<td>diagnose test application {wad</td>
<td>wa_cs</td>
</tr>
<tr>
<td>diagnose wadbd clear</td>
<td>Clear the WAN optimization database.</td>
</tr>
</tbody>
</table>
Peers and authentication groups

All communication between WAN optimization peers begins with one WAN optimization peer (or client-side FortiGate unit) sending a WAN optimization tunnel request to another peer (or server-side FortiGate unit). During this process, the WAN optimization peers identify and authenticate with each other.

This chapter describes:

- Basic WAN optimization peer authentication requirements
- How FortiGate units process tunnel requests for peer authentication
- Configuring peers
- Configuring authentication groups
- Secure tunneling

Basic WAN optimization peer authentication requirements

Peer authentication requires the following configuration on each peer for best results.

- All peers must have a unique host ID that identifies each peer. You can add the host ID to a peer from the web-based manager by going to WAN Opt. & Cache > Peer, entering a host ID in the Local Host ID field and selecting Apply. The host ID can contain up to 25 characters and can include spaces. Do not leave the host ID at its default value.

- All peers must know the host IDs and IP addresses of all of the other peers that they can start WAN optimization tunnels with. You add these host IDs and IP addresses from the web-based manager by going to WAN Opt. & Cache > Peer and selecting Create New. You then enter the other peer’s host ID in the Peer Host ID field, enter the other peer’s IP address in the IP Address field and select OK. The IP address will be the source IP address of tunnel requests sent by the peer. Usually this is the IP address of the peer’s interface that is connected to the WAN—the IP address of the interface from which tunnel requests are sent.

- All peers must have the same local certificate installed on their FortiGate units if the units authenticate by local certificate. Similarly, if the units authenticate by pre-shared key (password), administrators must know the password. For more information, see the FortiGate Certificate Management Guide.

Accepting any peers

Strictly speaking, you do not need to add peers. Instead you can configure authentication groups that accept any peer. However, for this to work, both peers must have the same authentication group (with the same name) and both peers must have the same certificate or pre-shared key.
Accepting any peer is useful if you have many peers or if peer IP addresses change. For example, you could have many travelling FortiClient peers with IP addresses that are always changing as the users travel to different customer sites. This configuration is also useful if you have FortiGate units with dynamic external IP addresses (using DHCP or PPPoE). For most other situations, this method is not recommended as it is less secure than accepting defined peers or a single peer. For more information, see “Configuring authentication groups” on page 32.

How FortiGate units process tunnel requests for peer authentication

When a client-side FortiGate unit attempts to start a WAN optimization tunnel with a peer server-side FortiGate unit, the tunnel request includes the following information:

• the client-side local host ID
• the name of an authentication group if included in the rule that initiates the tunnel
• the authentication method defined in the authentication group: pre-shared key or certificate
• the type of tunnel (secure or not).

For information about configuring the local host ID, peers and authentication groups, see “Configuring peers” on page 31 and “Configuring authentication groups” on page 32.

The authentication group is optional unless the tunnel is a secure tunnel. For more information, see “Secure tunneling” on page 34.

If the tunnel request includes an authentication group, the authentication will be based on the settings of this group as follows:

• The server-side FortiGate unit searches its own configuration for the name of the authentication group in the tunnel request. If no match is found, the authentication fails.
• If a match is found, the server-side FortiGate unit compares the authentication method in the client and server authentication groups. If the methods do not match, the authentication fails.
• If the authentication methods match, the server-side FortiGate unit tests the peer acceptance settings in its copy of the authentication group.
  • If the setting is Accept Any Peer, the authentication is successful.
  • If the setting is Specify Peer, the server-side FortiGate unit compares the client-side local host ID in the tunnel request with the peer name in the server-side authentication group. If the names match, authentication is successful. If a match is not found, authentication fails.
  • If the setting is Accept Defined Peers, the server-side FortiGate unit compares the client-side local host ID in the tunnel request with the server-side peer list. If a match is found, authentication is successful. If a match is not found, authentication fails.

If the tunnel request does not include an authentication group, authentication will be based on the client-side local host ID in the tunnel request. The server-side FortiGate unit searches its peer list to match the client-side local host ID in the tunnel request. If a match is found, authentication is successful. If a match is not found, authentication fails.

If the server-side FortiGate unit successfully authenticates the tunnel request, the server-side FortiGate unit sends back a tunnel setup response message. This message includes the server-side local host ID and the authentication group that matches the one in the tunnel request.
The client-side FortiGate unit then performs the same authentication procedure as the server-side FortiGate unit did. If both sides succeed, tunnel setup continues.

Configuring peers

When you configure peers, you first need to add the local host ID that identifies the FortiGate unit for WAN optimization and then add the peer host ID and IP address of each FortiGate unit with which a FortiGate unit can create WAN optimization tunnels.

**Figure 16: WAN optimization peer list**

![WAN optimization peer list](image)

To configure WAN optimization peers - web-based manager

1. Go to **Wan Opt. & Cache > Peer**.
2. For **Local Host ID**, enter the local host ID of this FortiGate unit and select **Apply**. If you add this FortiGate unit as a peer to another FortiGate unit, use this ID as its **peer** host ID.
3. Select **Create New** to add a new peer.
4. For **Peer Host ID**, enter the peer host ID of the peer FortiGate unit. This is the local host ID added to the peer FortiGate unit.
5. For **IP Address**, add the IP address of the FortiGate unit. Usually this is the IP address of the FortiGate interface connected to the WAN.
6. Select **OK**.

To configure WAN optimization peers - CLI

In this example, the local host ID is named **HQ_Peer** and has an IP address of **172.20.120.100**. Three peers are added, but you can add any number of peers that are on the WAN.

1. Enter the following command to set the local host ID to **HQ_Peer**.
   ```
   config wanopt settings
   set host-id HQ Peer
   end
   ```
2. Enter the following commands to add three peers.
   ```
   config wanopt peer
   edit Wan_opt_peer_1
   set ip 172.20.120.100
   next
   edit Wan_opt_peer_2
   ```
Configuring authentication groups

You need to add authentication groups to support authentication and secure tunneling between WAN optimization peers.

To perform authentication, WAN optimization peers use a certificate or a pre-shared key added to an authentication group so they can identify each other before forming a WAN optimization tunnel. Both peers must have an authentication group with the same name and settings. You add the authentication group to a peer-to-peer or active rule on the client-side FortiGate unit. When the server-side FortiGate unit receives a tunnel start request from the client-side FortiGate unit that includes an authentication group, the server-side FortiGate unit finds an authentication group in its configuration with the same name. If both authentication groups have the same certificate or pre-shared key, the peers can authenticate and set up the tunnel.

Authentication groups are also required for secure tunneling. See “Secure tunneling” on page 34.

To add authentication groups, go to WAN Opt. & Cache > Peer > Authentication Group.

![Figure 17: WAN optimization Authentication Group list](image)

### To add an authentication group - web-based manager

Use the following steps to add any kind of authentication group. It is assumed that if you are using a local certificate to authenticate, it is already added to the FortiGate unit. For more information, see the FortiGate Certificate Management Guide.

2. Select Create New.
3 Add a Name for the authentication group.
You will select this name when you add the authentication group to a WAN optimization rule.

4 Select the Authentication Method.
Select Certificate if you want to use a certificate to authenticate and encrypt WAN optimization tunnels. You must also select a local certificate that has been added to this FortiGate unit. (To add a local certificate, go to System > Certificates > Local Certificates.) Other FortiGate units that participate in WAN optimization tunnels with this FortiGate unit must have an authentication group with the same name and certificate.

Select Pre-shared key if you want to use a pre-shared key or password to authenticate and encrypt WAN optimization tunnels. You must also add a Password (or pre-shared key) used by the authentication group. Other FortiGate units that participate in WAN optimization tunnels with this FortiGate unit must have an authentication group with the same name and password. The password must contain at least 6 printable characters and should be known only by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.

5 Configure Peer Acceptance for the authentication group.
Select Accept Any Peer if you do not know the peer host IDs or IP addresses of the peers that will use this authentication group. This setting is most often used for WAN optimization with the FortiClient application or with FortiGate units that do not have static IP addresses, for example units that use DHCP.

Select Accept Defined Peers if you want to authenticate with peers added to the peer list only.

Select Specify Peer and select one of the peers added to the peer list to authenticate with the selected peer only.

For more information, see “Configuring peers” on page 31.

6 Select OK.

7 Add the authentication group to a WAN optimization rule to apply the authentication settings in the authentication group to the rule.

For more information, see “Configuring WAN optimization rules” on page 42.

To add an authentication group that uses a certificate - CLI
Enter the following command to add an authentication group that uses a certificate and can authenticate all peers added to the FortiGate unit configuration.

In this example, the authentication group is named auth_grp_1 and uses a certificate named Example_Cert.

```
config wanopt auth-group
edit auth_grp_1
  set auth-method cert
  set cert Example_Cert
  set peer-accept defined
end
```

To add an authentication group that uses a pre-shared key - CLI
Enter the following command to add an authentication group that uses a pre-shared key and can authenticate only the peer added to the authentication group.

```
```
In this example, the authentication group is named `auth_peer`, the peer that the group can authenticate is named `Server_net`, and the authentication group uses `123456` as the pre-shared key. In practice you should use a more secure pre-shared key.

```plaintext
config wanopt auth-group
edit auth_peer
  set auth-method psk
  set psk 123456
  set peer-accept one
  set peer Server_net
end
```

To add an authentication group that accepts WAN optimization connections from any peer - web-based manager

Add an authentication group that accepts any peer for situations where you do not have the Peer Host IDs or IP Addresses of the peers that you want to perform WAN optimization with. This setting is most often used for WAN optimization with the FortiClient application or with FortiGate units that do not have static IP addresses, for example units that use DHCP. An authentication group that accepts any peer is less secure than an authentication group that accepts defined peers or a single peer.

The example below sets the authentication method to Pre-shared key. You must add the same password to all FortiGate units using this authentication group.

2. Select Create New to add a new authentication group.
3. Configure the authentication group:

<table>
<thead>
<tr>
<th>Name</th>
<th>Specify any name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method</td>
<td>Pre-shared key</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a pre-shared key.</td>
</tr>
<tr>
<td>Peer Acceptance</td>
<td>Accept Any Peer</td>
</tr>
</tbody>
</table>

To add an authentication group that accepts WAN optimization connections from any peer - CLI

In this example, the authentication group is named `auth_grp_1`. It uses a certificate named `WAN_Cert` and accepts any peer.

```plaintext
config wanopt auth-group
edit auth_grp_1
  set auth-method cert
  set cert WAN_Cert
  set peer-accept any
end
```

Secure tunneling

You can configure WAN optimization rules to use AES-128bit-CBC SSL to encrypt the traffic in the WAN optimization tunnel. WAN optimization uses FortiASIC acceleration to accelerate SSL decryption and encryption of the secure tunnel. The secure tunnel uses the same TCP port as a non-secure tunnel (TCP port 7810).
To use secure tunneling, you must select *Enable Secure Tunnel* in a WAN optimization rule and add an authentication group. The authentication group specifies the certificate or pre-shared key used to set up the secure tunnel. You can add a new authentication group to support secure tunneling or you can use an authentication group that was already added for tunnel authentication. The *Peer Acceptance* setting of the authentication group does not affect secure tunneling.

The FortiGate units at each end of the secure tunnel must have the same authentication group with the same name and the same configuration, including the same pre-shared key or certificate. To use certificates you must install the same certificate on both FortiGate units.

For active-passive WAN optimization you select *Enable Secure Tunnel* only in the active rule. In peer-to-peer WAN optimization you select *Enable Secure Tunnel* in the WAN optimization rule on both FortiGate units. For information about active-passive and peer-to-peer WAN optimization, see "Configuring WAN optimization rules" on page 37.

For a secure tunneling configuration example, see "Example: Adding secure tunneling to an active-passive WAN optimization configuration" on page 57. Secure tunneling is also used in the configuration example: "Example: SSL offloading for a WAN optimization tunnel" on page 103.
Configuring WAN optimization rules

To configure WAN optimization, you add WAN optimization rules. Similar to firewall policies, when a FortiGate unit receives a connection packet, it analyzes the packet’s source address, destination address, and service (by destination port number), and attempts to locate a matching WAN optimization rule that decides how to optimize the traffic over the WAN. WAN optimization rules also apply features such as byte-caching and protocol optimization to optimized traffic.

You can add one of two types of WAN optimization rules: active-passive and peer-to-peer.

For **active-passive WAN optimization**, you add active rules to client-side FortiGate units and passive rules to server-side FortiGate units. A single passive rule can accept tunnel requests from multiple active rules, thus allowing you to simplify the server-side configuration by adding fewer rules. The configuration of the active rule enables WAN optimization features. The passive rule uses the configuration of the active rules, further simplifying the server-side configuration. The one exception is web caching, which is enabled in passive rules.

A **peer-to-peer WAN optimization** rule includes a peer host ID. WAN optimization sessions matched by a client-side peer-to-peer rule can only connect to the named server-side peer. When the client-side peer unit initiates a tunnel with the server-side peer, the packets that initiate the tunnel include extra information so that this server-side peer can determine that it is a peer-to-peer tunnel request. This extra information is required because the server-side peer does not require a WAN optimization rule; you just need to add the client peer host ID and IP address to the server-side FortiGate unit peer list.

This chapter describes:

- WAN optimization rules, firewall policies, and protection profiles
- WAN optimization transparent mode
- WAN optimization rule list
- WAN optimization address formats
- Configuring WAN optimization rules

WAN optimization rules, firewall policies, and protection profiles

The FortiGate unit applies firewall policies to communication sessions before WAN optimization rules. A WAN optimization rule can be applied to a packet only after the packet is accepted by a firewall policy. WAN optimization processes all sessions accepted by a firewall policy that also match a WAN optimization rule.

However, if the firewall policy includes a protection profile, communication sessions accepted by the policy are processed by the protection profile and not by WAN optimization. To apply WAN optimization to traffic that is accepted by a firewall policy containing a protection profile, you can use multiple FortiGate units or multiple VDOMs. You apply the protection profile in the first FortiGate unit or VDOM and then apply WAN optimization in the second FortiGate unit or VDOM. You also add inter-VDOM links between the VDOMs. See the configuration example “Out-of-path WAN optimization with inter-VDOM routing” on page 81.
WAN optimization does not apply source and destination NAT settings included in firewall policies. This means that selecting NAT or adding virtual IPs in a firewall policy does not affect WAN optimized traffic. WAN optimization is also not compatible with firewall load balancing. However, traffic accepted by these policies that is not WAN optimized is processed as expected.

WAN optimization is compatible with identity-based firewall policies. If a session is allowed after authentication and if the identity-based policy that allows the session does not include a protection profile, the session can be processed by matching WAN optimization rules.

Firewall traffic shaping is compatible with client/server (active-passive) transparent mode WAN optimization rules. Traffic shaping is ignored for peer-to-peer WAN optimization and for client/server WAN optimization not operating in transparent mode.

**WAN optimization transparent mode**

WAN optimization is transparent to users. This means that with WAN optimization in place, clients connect to servers in the same way as they would without WAN optimization. However, servers receiving packets after WAN optimization “see” different source addresses depending on whether or not transparent mode is selected for WAN optimization. If transparent mode is selected, WAN optimization keeps the original source address of the packets, so servers appear to receive traffic directly from clients. Routing on the server network should be configured to route traffic with client source IP addresses from the server-side FortiGate unit to the server and back to the server-side FortiGate unit.

**Note:** Some protocols, for example CIFS, may not function as expected if transparent mode is not selected. In most cases, for CIFS WAN optimization you should select transparent mode and make sure the server network can route traffic as described to support transparent mode.

If transparent mode is not selected, the source address of the packets received by servers is changed to the address of the server-side FortiGate unit interface that sends the packets to the servers. So servers appear to receive packets from the server FortiGate unit. Routing on the server network is simpler in this case because client addresses are not involved. All traffic appears to come from the server FortiGate unit and not from individual clients.

**Note:** Do not confuse WAN optimization transparent mode with FortiGate Transparent mode. WAN optimization transparent mode is configured in individual WAN optimization rules. FortiGate Transparent mode is a system setting that controls how the FortiGate unit (or a VDOM) processes traffic.

**WAN optimization rule list**

The WAN optimization rule list displays WAN optimization rules in their order of matching precedence. You can add, delete, edit, and re-order rules in the rule list. WAN optimization rule order affects rule matching. For details about arranging rules in the rule list, see "How list order affects rule matching" on page 40 and "Moving a rule to a different position in the rule list" on page 41.

Before you add WAN optimization rules, you must add firewall policies to accept the traffic that you want to optimize. For information about WAN optimization rules and firewall policies, see “WAN optimization rules, firewall policies, and protection profiles” on page 37.
Then you add WAN optimization rules that:

- match WAN traffic to be optimized that is accepted by a firewall policy according to source and destination addresses and destination port of the traffic
- add the WAN optimization techniques to be applied to the traffic.

To view the WAN optimization rule list, go to **WAN Opt. & Cache > Rule**.

**Figure 18: WAN optimization rule list**

<table>
<thead>
<tr>
<th>Status</th>
<th>ID</th>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Method</th>
<th>Auto-Detect</th>
<th>Peer</th>
<th>Mode</th>
<th>SSL</th>
<th>Secure Tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2.1.1.1</td>
<td>2.4.2.2</td>
<td>1</td>
<td>68-26</td>
<td>Byte Caching</td>
<td>Off</td>
<td>CIFS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>10.1.100.*</td>
<td>172.16.200.*</td>
<td>89-89</td>
<td>Byte Caching</td>
<td>Active</td>
<td>HTTP</td>
<td>Full Optimization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>10.1.100.*</td>
<td>12.0.0.0-0.0.0.255</td>
<td>123-</td>
<td>Active</td>
<td>MAN</td>
<td>Full Optimization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>10.1.100.*</td>
<td>172.16.200.*</td>
<td>21-21</td>
<td>Byte Caching</td>
<td>Active</td>
<td>FTP</td>
<td>Full Optimization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>10.1.100.*</td>
<td>172.16.200.*</td>
<td>129-</td>
<td>Byte Caching</td>
<td>Active</td>
<td>CIFS</td>
<td>Full Optimization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>10.1.100.*</td>
<td>172.16.200.*</td>
<td>445-</td>
<td>Byte Caching</td>
<td>Active</td>
<td>HTTPS</td>
<td>Full Optimization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>10.1.100.*</td>
<td>172.16.200.*</td>
<td>443-</td>
<td>Byte Caching</td>
<td>Active</td>
<td>HTTP</td>
<td>Full Optimization</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Create New**

Add a new WAN optimization rule. New rules are added to the bottom of the list.

**Status**

Select to enable a rule or clear to disable a rule. A disabled rule is out of service.

**ID**

The rule identifier. Rules are numbered in the order they are added to the rule list.

**Source**

The source address or address range that the rule matches. For more information, see "WAN optimization address formats" on page 42.

**Destination**

The destination address or address range that the rule matches. For more information, see "WAN optimization address formats" on page 42.

**Port**

The destination port number or port number range that the rule matches.

**Method**

Indicates whether you have selected byte caching in the WAN optimization rule.

**Auto-Detect**

Indicates whether the rule is an active (client) rule, a passive (server) rule or if auto-detect is off. If auto-detect is off, the rule can be peer-to-peer or Web Cache Only.

**Protocol**

The protocol optimization WAN optimization technique applied by the rule. For more information, see "Protocol optimization" on page 24.

**Peer**

For a peer-to-peer rule, the name of the peer WAN optimizer at the other end of the link.

**Mode**

Indicates whether the rule applies Full Optimization or Web Cache Only.

**SSL**

Indicates whether the rule is configured for SSL offloading.

**Secure Tunnel**

Indicates whether the rule is configured to used a WAN optimization tunnel.

**Delete icon**

Delete a rule from the list.

**Edit icon**

Edit a rule.
How list order affects rule matching

Similar to firewall policies, you add WAN optimization rules to the WAN optimization rule list. The FortiGate unit uses the first-matching technique to select the WAN optimization rule to apply to a communication session.

When WAN optimization rules have been added, each time the FortiGate firewall accepts a communication session, it then searches the WAN optimization rule list for a matching rule. The search begins at the top of the rule list and progresses in order towards the bottom. Each rule in the rule list is compared with the communication session until a match is found. When the FortiGate unit finds the first matching rule, it applies that rule’s specified WAN optimization features to the session and disregards subsequent rules. Matching rules are determined by comparing the rule with the session source, destination addresses and destination port.

If no WAN optimization rule matches, the session is processed according to the firewall policy that originally accepted the session.

As a general rule, you should order the WAN optimization rule list from most specific to most general because of the order in which rules are evaluated for a match, and because only the first matching rule is applied to a session. Subsequent possible matches are not considered or applied. Ordering rules from most specific to most general prevents rules that match a wide range of traffic from superseding and effectively masking rules that match exceptions.

For example, you might have a general WAN optimization rule that applies WAN optimization features but does not apply secure tunneling to most WAN traffic; however, you want to apply secure tunneling to FTP traffic (FTP traffic uses port 21). In this case, you would add a rule that creates a secure tunnel for FTP sessions above the general rule.

Figure 19: Example: secure tunneling for FTP — correct rule order

FTP sessions (using port 21) would immediately match the secure tunnel rule. Other kinds of services would not match the FTP rule, so rule evaluation would continue until the search reaches the matching general rule. This rule order has the intended effect. But if you reversed the order of the two rules, positioning the general rule before the FTP rule, all session, including FTP, would immediately match the general rule, and the rule to secure FTP would never be applied. This rule order would not have the intended effect.
Configuring WAN optimization rules

WAN optimization rule list

Figure 20: Example: secure tunneling for FTP — incorrect rule order

Similarly, if specific traffic requires exceptional WAN optimization rule settings, you would position those rules above other potential matches in the rule list. Otherwise, the other matching rules would take precedence, and the required exceptional settings might never be used.

Moving a rule to a different position in the rule list

You can arrange the WAN optimization rule list to influence the order in which rules are evaluated for matches with incoming traffic. When more than one rule has been defined, the first matching rule will be applied to the traffic session. For more information, see "How list order affects rule matching" on page 40.

Moving a rule in the rule list does not change its ID, which only indicates the order in which the rule was created.

Figure 21: Move rule

To move a rule in the WAN optimization rule list - web-based manager

2. In the rule list, note the ID of a rule that is before or after your intended destination.
3. In the row corresponding to the rule that you want to move, select the Move To icon.
4. Select Before or After, and enter the ID of the rule that is before or after your intended destination. This specifies the rule’s new position in the WAN optimization rule list.
5. Select OK.

To move a rule in the WAN optimization rule list - CLI

1. Use the following command to move a WAN optimization rule with ID 34 above the rule in the rule list with ID 10.
   ```
   config wanopt rule
   move 34 before 10
   end
   ```
2. Use the following command to move a WAN optimization rule with ID 5 after the rule in the rule list with ID 1.
   ```
   config wanopt rule
   move 5 after 1
   end
   ```
WAN optimization address formats

A WAN optimization source or destination address can contain one or more network addresses. Network addresses can be represented by an IP address with a netmask or an IP address range.

When representing hosts by an IP address with a netmask, the IP address can represent one or more hosts. For example, a source or destination address can be:

- a single computer, for example, 192.45.46.45
- a subnetwork, for example, 192.168.1.* for a class C subnet
- 0.0.0.0, matches any IP address.

The netmask corresponds to the subnet class of the address being added, and can be represented in either dotted decimal or CIDR format. The FortiGate unit automatically converts CIDR-formatted netmasks to dotted decimal format. Example formats:

- netmask for a single computer: 255.255.255.255, or /32
- netmask for a class A subnet: 255.0.0.0, or /8
- netmask for a class B subnet: 255.255.0.0, or /16
- netmask for a class C subnet: 255.255.255.0, or /24
- netmask including all IP addresses: 0.0.0.0

Valid IP address and netmask formats include:

- x.x.x.x/x.x.x.x, such as 192.168.1.0/255.255.255.0
- x.x.x.x/x, such as 192.168.1.0/24

Note: An IP address 0.0.0.0 with netmask 255.255.255.255 is not a valid source or destination address.

When representing hosts by an IP range, the range indicates hosts with continuous IP addresses in a subnet, such as 192.168.1.[2-10], or 192.168.1.* to indicate the complete range of hosts on that subnet. You can also indicate the complete range of hosts on a subnet by entering 192.168.1.0-192.168.1.255. Valid IP range formats include:

- x.x.x.x-x.x.x.x, for example, 192.168.110.100-192.168.110.120
- x.x.x.[x-x], for example, 192.168.110.[100-120]
- x.x.x.*, for a complete subnet, for example: 192.168.110.*
- x.x.x.[0-255] for a complete subnet, such as 192.168.110.[0-255]
- x.x.x.0 -x.x.x.255 for a complete subnet, such as 192.168.110.0 - 192.168.110.255

Note: You cannot use square brackets [] or asterisks * when adding addresses to the CLI. Instead you must enter the start and end addresses of the subnet range separated by a dash -. For example, 192.168.20.0-192.168.20.255 for a complete subnet and 192.168.10.10-192.168.10.100 for a range of addresses.

Configuring WAN optimization rules

This section describes all the details that you can configure for the WAN optimization rules. The options available depend on how you configure a specific rule. The conditions are noted.
To add a WAN optimization rule - web-based manager

1. Go to **WAN Opt. & Cache > Rule** and select **Create New**.
2. Configure the WAN optimization rule, using the guidance in the following table, and select **OK**.

### Mode
- Select **Full Optimization** to add a rule that can apply all WAN optimization features.
- Select **Web Cache Only** to add a rule that just applies web caching. If you select **Web Cache Only**, you can configure the source and destination address and port for the rule. You can also select **Transparent Mode** and **Enable SSL**.

### Source
- Enter an IP address, followed by a forward slash (/), then subnet mask, or enter an IP address range separated by a hyphen. For more information, see "WAN optimization address formats" on page 42.
- Only packets whose source address header contains an IP address matching this IP address or address range will be accepted by and subject to this rule.
- **Tip:** For a Web Cache Only rule, if you set **Destination** to 0.0.0.0, the rule caches web pages on the Internet or any network.

### Destination
- Enter an IP address, followed by a forward slash (/), then subnet mask, or enter an IP address range separated by a hyphen. For more information, see "WAN optimization address formats" on page 42.
- Only a packet whose destination address header contains an IP address matching this IP address or address range will be accepted by and subject to this rule.
- **Tip:** For a Web Cache Only rule, if you set **Destination** to 0.0.0.0, the rule caches web pages on the Internet or any network.

### Port
- Enter a single port number or port number range. Only packets whose destination port number matches this port number or port number range will be accepted by and subject to this rule.
- **Tip:** For a Web Cache Only rule, if you set **Destination** to 0.0.0.0, the rule caches web pages on the Internet or any network.

---

**Figure 22: Configuring a WAN optimization rule**

<table>
<thead>
<tr>
<th>New Wan Optimization Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
</tr>
<tr>
<td><strong>Source</strong></td>
</tr>
<tr>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td><strong>Port</strong></td>
</tr>
<tr>
<td><strong>Auto-Detect</strong></td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
</tr>
<tr>
<td><strong>Peer</strong></td>
</tr>
<tr>
<td><strong>Enable Web Cache</strong></td>
</tr>
<tr>
<td><strong>Transparent Mode</strong></td>
</tr>
<tr>
<td><strong>Enable Byte Caching</strong></td>
</tr>
<tr>
<td><strong>Enable SSL</strong></td>
</tr>
<tr>
<td><strong>Enable Secure Tunnel</strong></td>
</tr>
<tr>
<td><strong>Authentication Group</strong></td>
</tr>
</tbody>
</table>

**OK** | **Cancel**
### Auto-Detect
Available only if Mode is set to **Full Optimization**.
Specify whether the rule is **Active** (client), **Passive** (server) or if **Auto-Detect** is **Off**.
If **Auto-Detect** is **Off**, the rule is a peer-to-peer rule.
- For an **Active** (client) rule, you must select all of the WAN optimization features to be applied by the rule. You can select the protocol to optimize, transparent mode, byte caching, SSL offloading, secure tunneling, and an authentication group.
- A **Passive** (server) rule uses the settings in the active rule on the client FortiGate unit to apply WAN optimization settings. You can also select web caching for a passive rule.
- If **Auto-Detect** is **Off**, the rule must include all required WAN optimization features and you must select a **Peer** for the rule. Select this option to configure peer-to-peer WAN optimization where this rule can start a WAN optimization tunnel with this peer only.

### Protocol
Available only if Mode is set to **Full Optimization**, and **Auto-Detect** is set to **Off** or **Active**.
Select CIFS, FTP, HTTP, or MAPI to apply protocol optimization for one of these protocols. For information about protocol optimization, see “Protocol optimization” on page 24.
Select TCP if the WAN optimization tunnel accepts sessions that use more than one protocol or that do not use the CIFS, FTP, HTTP, or MAPI protocol.

### Peer
Available only if Mode is set to **Full Optimization**, and **Auto-Detect** is set to **Off**.
Select the peer host ID of the peer that this peer-to-peer WAN optimization rule will start a WAN optimization tunnel with. You can also select [Create New...] from the list to add a new peer.

### Enable Web Cache
Available only if Mode is set to **Full Optimization**, and **Auto-Detect** is set to **Off** or **Passive**. If **Auto-Detect** is set to **Off**, then **Protocol** must be set to **HTTP**.
Select to apply WAN optimization web caching to the sessions accepted by this rule. For more information, see “Web caching” on page 63.

### Transparent Mode
Available only if Mode is set to **Full Optimization** and **Auto-Detect** is set to **Active** or **Off**, or if **Mode** is set to **Web Cache Only**.
Servers receiving packets after WAN optimization “see” different source addresses depending on whether or not you select **Transparent Mode**.
For more information, see “WAN optimization transparent mode” on page 38.

### Enable Byte Caching
Available only if Mode is set to **Full Optimization**, and **Auto-Detect** is set to **Off** or **Active**.
Select to apply WAN optimization byte caching to the sessions accepted by this rule. For more information, see “Byte caching” on page 25.

### Enable SSL
Available only if **Auto-Detect** is set to **Active** or **Off**.
Select to apply SSL offloading for HTTPS traffic. You can use SSL offloading to offload SSL encryption and decryption from one or more HTTP servers to the FortiGate unit. If you enable this option, you must configure the rule to accept SSL-encrypted traffic. For example, you can configure the rule to accept HTTPS traffic by setting **Port** to 443.
If you enable SSL offloading, you must also use the CLI command `config wanopt ssl-server` to add an SSL server for each HTTP server that you want to offload SSL encryption/decryption for. For more information, see “SSL offloading for WAN optimization and web caching” on page 103.

### Enable Secure Tunnel
Available only if Mode is set to **Full Optimization**, and **Auto-Detect** is set to **Active** or **Off**.
If you select **Enable Secure Tunnel**, the WAN optimization tunnel is encrypted using SSL encryption. You must also add an authentication group to the rule. For more information, see “Secure tunneling” on page 34.

### Authentication Group
Available only if Mode is set to **Full Optimization**, and **Auto-Detect** is set to **Active** or **Off**.
Select this option and select an authentication group from the list if you want groups of FortiGate units to authenticate with each other before starting the WAN optimization tunnel. You must also select an authentication group if you select **Enable Secure Tunnel**.
You must add identical authentication groups to both of the FortiGate units that will participate in the WAN optimization tunnel started by the rule. For more information, see “Configuring authentication groups” on page 32.
To add a WAN optimization rule - CLI

Using the guidance in the previous table, enter the following commands. For more information, see the wanopt and rules listings in the FortiGate CLI Reference.

```
config wanopt rule
edit <index_int>
    set auth-group <auth_group_name>
    set auto-detect {active | off | passive}
    set byte-caching {disable | enable}
    set dst-ip <address_ipv4>[-<address-ipv4>]
    set mode {full | webcache-only}
    set peer <peer_name>
    set port <port_int>[-<port-int>]
    set proto {cifs | ftp | http | mapi | tcp}
    set secure-tunnel {disable | enable}
    set src-ip <address_ipv4>[-<address-ipv4>]
    set ssl {disable | enable}
    set status {disable | enable}
    set transparent {disable | enable}
    set tunnel-non-http {disable | enable}
    set tunnel-sharing {express-shared | private | shared}
    set unknown-http-version {best-effort | reject | tunnel}
    set webcache {disable | enable}
end
```

Processing non-HTTP sessions accepted by an HTTP rule

From the CLI, use the tunnel-non-http keyword of the config wanopt rule command to configure how to process non-HTTP sessions when a rule configured to accept and optimize HTTP traffic accepts a non-HTTP session. This can occur if an application sends non-HTTP sessions using an HTTP destination port.

You can set tunnel-non-http to disable to drop non-HTTP sessions accepted by the rule or you can set it to enable to pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. In this case, the FortiGate unit applies TCP protocol optimization to non-HTTP sessions.

Processing unknown HTTP sessions

Unknown HTTP sessions are HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1. From the CLI, use the unknown-http-version keyword of the config wanopt rule command to specify how a rule handles such HTTP sessions.

You can select best-effort to assume that all HTTP sessions accepted by the rule comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, WAN optimization may not parse it correctly. As a result, the FortiGate unit may stop forwarding the session and the connection may be lost.

You can select reject to reject HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.

You can also select tunnel to pass HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1, but without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied to these HTTP sessions.
WAN optimization configuration examples

This chapter provides the following basic examples to illustrate WAN optimization configurations introduced in the previous chapters:

- Example: Basic active-passive WAN optimization
- Example: Basic peer-to-peer WAN optimization configuration
- Example: Adding secure tunneling to an active-passive WAN optimization configuration

Example: Basic active-passive WAN optimization

In active-passive WAN optimization you add active WAN optimization rules on the client-side FortiGate unit by setting WAN optimization Auto-Detect to Active. You configure passive WAN optimization rules on the server-side FortiGate unit by setting WAN optimization Auto-Detect to Passive.

You can add multiple active rules for one passive rule to optimize different protocols. Since you do not configure the protocol in the passive rule, one passive rule can be used for each of the active rules. Adding fewer passive rules simplifies the WAN optimization configuration.

Network topology and assumptions

This example configuration includes three active rules on the client-side FortiGate unit and one passive rule in the server-side FortiGate unit. The active rules do the following:

- optimize CIFS traffic from IP addresses 172.20.120.100 to 172.20.120.200
- optimize HTTP traffic from IP addresses 172.20.120.100 to 172.20.120.150
- optimize FTP traffic from IP addresses 172.20.120.151 172.20.120.200.

You can do this by adding three active WAN optimization rules to the client-side FortiGate unit, one for each protocol—with port set to 80 for the HTTP rule, 21 for the FTP rule and 1-65535 for the CIFS rule. Then you arrange the rules in the WAN optimization rule list with the CIFS rule last because the HTTP and FTP rules include single port numbers.
General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the client-side FortiGate unit by adding peers and a firewall policy that accepts traffic to be optimized.
2. Add WAN optimization rules to the FortiGate unit.
3. Configure the server-side FortiGate unit.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

Configuring basic active-passive WAN optimization - web-based manager

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit web-based manager. (CLI steps follow.)

To configure peers on the client-side FortiGate unit and add a firewall policy

1. Go to WAN Opt. & Cache > Peer and enter a Local Host ID for the client-side FortiGate unit:

   Local Host ID: User_net

2. Select Apply to save your setting.
3 Select Create New and add a Peer Host ID and the IP Address for the server-side FortiGate unit:

<table>
<thead>
<tr>
<th>Peer Host ID</th>
<th>Web_servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.20.1</td>
</tr>
</tbody>
</table>

4 Select OK.

5 Go to Firewall > Policy and select Create New to add a firewall policy to the client-side FortiGate unit to accept the traffic to be optimized:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port2</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>ANY</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

To add the active rules to the client-side FortiGate unit

1 Go to WAN Opt. & Cache > Rule.

2 Select Create New to add the active rule to optimize CIFS traffic from IP addresses 172.20.120.100 to 172.20.120.200:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Full Optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>172.20.120.[100-200]</td>
</tr>
<tr>
<td>Destination</td>
<td>192.168.10.*</td>
</tr>
<tr>
<td>Port</td>
<td>1 - 65535</td>
</tr>
<tr>
<td>Auto-Detect</td>
<td>Active</td>
</tr>
<tr>
<td>Protocol</td>
<td>CIFS</td>
</tr>
<tr>
<td>Transparent Mode</td>
<td>Select</td>
</tr>
<tr>
<td>Enable Byte Caching</td>
<td>Select</td>
</tr>
</tbody>
</table>

3 Select OK.

4 Select Create New to add the active rule to optimize HTTP traffic for IP addresses 172.20.120.100 to 172.20.120.150:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Full Optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>172.20.120.[100-150]</td>
</tr>
<tr>
<td>Destination</td>
<td>192.168.10.*</td>
</tr>
<tr>
<td>Port</td>
<td>80</td>
</tr>
<tr>
<td>Auto-Detect</td>
<td>Active</td>
</tr>
<tr>
<td>Protocol</td>
<td>HTTP</td>
</tr>
<tr>
<td>Transparent Mode</td>
<td>Select</td>
</tr>
<tr>
<td>Enable Byte Caching</td>
<td>Select</td>
</tr>
</tbody>
</table>

5 Select OK.
6 Select Create New to add the active rule to optimize FTP traffic from IP addresses 172.20.120.151 - 172.20.120.200:

- **Mode**: Full Optimization
- **Source**: 172.20.120.[151-200]
- **Destination**: 192.168.10.*
- **Port**: 21
- **Auto-Detect**: Active
- **Protocol**: FTP
- **Transparent Mode**: Select
- **Enable Byte Caching**: Select

7 Select OK.

8 If required, use the Move To icon to change the order of the rules in the list so that the HTTP and FTP rules are above the CIFS rule in the list. You may need to do this if you have other WAN optimization rules in the list.

For more information, see "How list order affects rule matching" on page 40 and "Moving a rule to a different position in the rule list" on page 41.

Figure 25: HTTP, FTP, and CIFS rules in the rule list

To configure the server-side FortiGate unit

1 Go to **WAN Opt. & Cache > Peer** and enter a **Local Host ID** for the server-side FortiGate unit:

   - **Local Host ID**: Web_servers

2 Select Apply to save your setting.

3 Select Create New and add a **Peer Host ID** and the **IP Address** for the client-side FortiGate unit:

   - **Peer Host ID**: User_net
   - **IP Address**: 172.30.120.1

4 Select OK.

5 Go to **WAN Opt. & Cache > Rule** and select Create New.

6 Add the passive rule. The source address matches the 172.20.120.100 to 172.20.120.200 IP address range and the 1-65535 port range. You can also enable web caching for the HTTP traffic:

- **Mode**: Full Optimization
- **Source**: 172.20.120.[100-200]
- **Destination**: 192.168.10.*
WAN optimization configuration examples

Example: Basic active-passive WAN optimization

Figure 26: Example passive rule

<table>
<thead>
<tr>
<th>Port</th>
<th>1-65535</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Detect</td>
<td>Passive</td>
</tr>
<tr>
<td>Enable Web Cache</td>
<td>Select</td>
</tr>
</tbody>
</table>

7. Select OK.
   The rule is added to the bottom of the rule list.

8. If required, move the rule to a different position in the list so that the tunnel request from the client-side FortiGate unit matches with this rule.

For more information, see “Moving a rule to a different position in the rule list” on page 41.

Configuring basic active-passive WAN optimization - CLI

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit CLI.

To configure peers on the client-side FortiGate unit and add a firewall policy

1. Add the Local Host ID to the client-side FortiGate configuration:
   ```
   config wanopt settings
   set host-id User_net
   end
   ```

2. Add the server-side Local Host ID to the client-side peer list:
   ```
   config wanopt peer
   edit Web_servers
   set ip 192.168.20.1
   end
   ```

3. Add a firewall policy to the client-side FortiGate unit to accept the traffic to be optimized:
   ```
   config firewall policy
   edit 20
   set srcintf port1
   set dstintf port2
   set srcaddr all
   set dstaddr all
   set action accept
   set service ANY
   set schedule always
   end
   ```
To add the active rules to the client-side FortiGate unit

1. Add the following active rule to optimize CIFS traffic for IP addresses 172.20.120.100 to 172.20.120.200:

   ```
   config wanopt rule
   edit 2
   set auto-detect active
   set src-ip 172.20.120.100-172.20.120.200
   set dst-ip 192.168.10.0-192.168.10.255
   set port 1-65535
   set proto cifs
   end
   ```

   Accept default settings for:
   - transparent (enable)
   - status (enable)
   - mode (full)
   - byte-caching (enable)
   - ssl (disable)
   - secure-tunnel (disable)
   - auth-group (null)
   - unknown-http-version (tunnel)
   - and tunnel-non-http (disable).

2. Add the following active rule to optimize HTTP traffic for IP addresses 172.20.120.100 to 172.20.120.150:

   ```
   config wanopt rule
   edit 3
   set auto-detect active
   set src-ip 172.20.120.100-172.20.120.150
   set dst-ip 192.168.10.0-192.168.10.255
   set port 80
   end
   ```

   Accept default settings for:
   - transparent (enable)
   - proto (http)
   - status (enable)
   - mode (full)
   - byte-caching (enable)
   - ssl (disable)
   - secure-tunnel (disable)
   - auth-group (null)
   - unknown-http-version (tunnel)
   - and tunnel-non-http (disable).

3. Add the following active rule to optimize FTP traffic from IP addresses 172.20.120.151 to 172.20.120.200:

   ```
   config wanopt rule
   edit 4
   set auto-detect active
   set src-ip 172.20.120.151-172.20.120.200
   set dst-ip 192.168.10.0-192.168.10.255
   set port 21
   set proto ftp
   end
   ```

   Accept default settings for:
   - transparent (enable)
   - status (enable)
   - mode (full)
   - byte-caching (enable)
   - ssl (disable)
   - secure-tunnel (disable)
   - auth-group (null)
   - unknown-http-version (tunnel)
   - and tunnel-non-http (disable).

4. If required, use the move command to change the order of the rules in the list so that the HTTP and FTP rules are above the CIFS rule in the list. You may need to do this if you have other WAN optimization rules in the list.

   For more information, see "How list order affects rule matching" on page 40 and "Moving a rule to a different position in the rule list" on page 41.

To configure the server-side FortiGate unit

1. Add the Local Host ID to the server-side FortiGate configuration:
config wanopt settings
    set host-id Web_servers
end

2 Add the client-side Local Host ID to the server-side peer list:

config wanopt peer
    edit User_net
    set ip 172.20.120.1
end

3 Add the following passive rule to the server-side FortiGate unit:

config wanopt rule
    edit 5
    set auto-detect passive
    set src-ip 172.20.120.[100-200]
    set dst-ip 192.168.10.0-192.168.10.255
    set port 1-65535
    set webcache enable
end

Accept default settings for status (enable) and mode (full).

4 If required, use the move command to move the rule to a different position in the list so that the tunnel request from the client-side FortiGate unit matches with this rule.

For more information, see “Moving a rule to a different position in the rule list” on page 41.

Example: Basic peer-to-peer WAN optimization configuration

Peer-to-peer WAN optimization is very similar to active-passive WAN optimization. The difference is that the peer-to-peer tunnel can be set up only between the client-side FortiGate unit and the server-side FortiGate unit named in the WAN optimization rule added to the client-side FortiGate unit. When the client-side FortiGate unit initiates a tunnel with the server-side FortiGate unit, the packets that initiate the tunnel include extra information so that this server-side FortiGate unit can determine that it is a peer-to-peer tunnel request. This extra information is required because the server-side FortiGate unit does not require a WAN optimization rule; you just need to add the client peer host ID and IP address to the server-side FortiGate unit peer list.

The extra information in the communication session plus the peer list entry allow the server-side FortiGate unit to set up the WAN optimization tunnel with the client-side FortiGate unit by using only the settings on the client-side WAN optimization rule.

Note: Traffic shaping is ignored for peer-to-peer WAN optimization.

In a peer-to-peer WAN optimization configuration you create a peer-to-peer WAN optimization rule on the client-side FortiGate unit with Auto-Detect to Off and include the peer host ID of the server-side FortiGate unit. Using this rule, the client-side FortiGate unit can create a WAN optimization tunnel only with the peer that is added to the rule.

You do not have to add a rule to the server-side FortiGate unit. But the server-side FortiGate unit peer list must include the client FortiGate unit. The server-side FortiGate unit uses the WAN optimization settings in the client-side rule.
Network topology and assumptions

This example configuration includes a client-side FortiGate unit called Peer_Fgt_1 with a WAN IP address of 172.20.34.12. This unit is in front of a network with IP address 172.20.120.0. The server-side FortiGate unit is called Peer_Fgt_2 with a WAN IP address of 192.168.30.12. This unit is in front of a web server network with IP address 192.168.10.0.

Figure 27: Example peer-to-peer topology

General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the client-side FortiGate unit by adding peers and a firewall policy that accepts traffic to be optimized.

2. Configure the server-side FortiGate unit.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

Configuring basic peer-to-peer WAN optimization - web-based manager

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit web-based manager. (CLI steps follow.)

Figure 28: Adding a peer-to-peer WAN optimization rule
To configure the client-side FortiGate unit and firewall policy

1. Go to WAN Opt. & Cache > Peer and enter a Local Host ID for the client-side FortiGate unit:

   Local Host ID Peer_Fgt_1

2. Select Apply to save your setting.

3. Select Create New and add a Peer Host ID and the IP Address for the server-side FortiGate unit:

   Peer Host ID Peer_Fgt_2
   IP Address 192.168.30.12

4. Select OK.

5. Go to Firewall > Policy and add a firewall policy to the client-side FortiGate unit that accepts traffic to be optimized:

   Source Interface/Zone port1
   Source Address all
   Destination Interface/Zone port2
   Destination Address all
   Schedule always
   Service ANY
   Action ACCEPT


7. Configure the rule:

   Mode Full Optimization
   Source 172.20.120.*
   Destination 192.168.10.*
   Port 1-65535
   Auto-Detect Off
   Protocol MAPI
   Peer Peer_Fgt_2
   Transparent Mode Select
   Enable Byte Caching Select

8. Select OK.

   The rule is added to the bottom of the WAN optimization list.

9. If required, move the rule to a different position in the list so that the rule accepts the required MAPI sessions. Depending on your rule list configuration, this may involve moving the rule above more general rules that would also match MAPI traffic.

   For more information, see “How list order affects rule matching” on page 40 and “Moving a rule to a different position in the rule list” on page 41.
To configure the server-side FortiGate unit
1. Go to WAN Opt. & Cache > Peer and enter a Local Host ID for the server-side FortiGate unit:
   - Local Host ID: Peer_Fgt_2
2. Select Apply to save your setting.
3. Select Create New and add a Peer Host ID and the IP Address for the peer side FortiGate unit:
   - Peer Host ID: Peer_Fgt_1
   - IP Address: 172.20.34.12
4. Select OK.

Configuring basic peer-to-peer WAN optimization - CLI

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit CLI.

To configure the client-side FortiGate unit and firewall policy
1. Add the Local Host ID to the client-side FortiGate configuration:
   ```
   config wanopt settings
   set host-id Peer_Fgt_1
   end
   ```
2. Add the server-side Local Host ID to the client-side peer list:
   ```
   config wanopt peer
   edit Peer_Fgt_2
   set ip 192.168.30.12
   end
   ```
3. Add a firewall policy to the client-side FortiGate unit to accept the traffic to be optimized:
   ```
   config firewall policy
   edit 23
   set srcintf port1
   set dstintf port2
   set srcaddr all
   set dstaddr all
   set action accept
   set service ANY
   set schedule always
   end
   ```
4. Add the following peer-to-peer rule:
   ```
   config wanopt rule
   edit 2
   set src-ip 172.20.120.0-172.20.120.255
   set dst-ip 192.168.10.0-192.168.10.255
   set port 1-65535
   set proto mapi
   set peer Peer_Fgt_2
   ```
WAN optimization configuration examples

Example: Adding secure tunneling to an active-passive WAN optimization configuration

This example shows how to configure two FortiGate units for active-passive WAN optimization with secure tunneling. The same authentication group is added to both FortiGate units. The authentication group includes a password (or pre-shared key) and has Peer Acceptance set to Accept any Peer. An active rule is added to the client-side FortiGate unit and a passive rule to the server-side FortiGate unit. The active rule uses secure tunneling, optimizes HTTP traffic, and uses Transparent Mode and byte caching.

The authentication group is named Auth_Secure_Tunnel and the password for the pre-shared key is 2345678. The topology for this example is shown in Figure 29. This example includes web-based manager configuration steps followed by equivalent CLI configuration steps. For information about secure tunneling, see “Secure tunneling” on page 34.

Network topology and assumptions

This example configuration includes a client-side FortiGate unit called User_net with a WAN IP address of 172.30.120.1. This unit is in front of a network with IP address 172.20.120.0. The server-side FortiGate unit is called Web_servers and has a WAN IP address of 192.168.20.1. This unit is in front of a web server network with IP address 192.168.10.0.

end

Accept default settings for auto-detect (off), transparent (enable), status (enable), mode (full), byte-caching (enable), ssl (disable), secure-tunnel (disable), auth-group (null), unknown-http-version (tunnel), and tunnel-non-http (disable).

5 If required, move the rule to a different position in the list.

For more information, see “Moving a rule to a different position in the rule list” on page 41.

6 If required, use the move command to change the order of the rules in the list so that the rule accepts the required MAPI sessions. Depending on your rule list configuration, this may involve moving the rule above more general rules that would also match MAPI traffic.

For more information, see “How list order affects rule matching” on page 40 and “Moving a rule to a different position in the rule list” on page 41.

To configure the server-side FortiGate unit

1 Add the Local Host ID to the server-side FortiGate configuration:
   config wanopt settings
   set host-id Peer_Fgt_2
   end

2 Add the client-side Local Host ID to the server-side peer list:
   config wanopt peer
   edit Peer_Fgt_1
   set ip 192.168.30.12
   end
General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the client-side FortiGate unit by adding peers and a firewall policy that accepts traffic to be optimized.
2. Add an authentication group and WAN optimization rule to the client-side FortiGate unit.
3. Configure peers on the server-side FortiGate unit.
4. Add the same authentication group and add a WAN optimization rule to the server-side FortiGate unit.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

Configuring WAN optimization with secure tunneling - web-based manager

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit web-based manager. (CLI steps follow.)

To configure peers on the client-side FortiGate unit and add a firewall policy

1. Go to WAN Opt. & Cache > Peer and enter a Local Host ID for the client-side FortiGate unit:

   Local Host ID User_net

2. Select Apply to save your setting.

3. Select Create New and add a Peer Host ID and the IP Address for the server-side FortiGate unit:

   Peer Host ID Web_servers
   IP Address 192.168.20.1

4. Select OK.

5. Go to Firewall > Policy and select Create New to add a firewall policy to the client-side FortiGate unit to accept the traffic to be optimized:

   Source Interface/Zone port1
   Source Address all
To add the authentication group and WAN optimization rule to the client-side FortiGate unit

1 Go to *Wan Opt. & Cache > Peer > Authentication Group*.
2 Select *Create New* to add a new authentication group to be used for secure tunneling:
   - **Name**: Auth_Secure_Tunnel
   - **Authentication Method**: Pre-shared key
   - **Password**: 2345678
   - **Peer Acceptance**: Accept Any Peer
3 Select *OK*.
4 Go to *Wan Opt. & Cache > Rule*.
5 Select *Create New* to add an active rule that enables secure tunneling and includes the authentication group:
   - **Mode**: Full Optimization
   - **Source**: 172.20.120.[100-200]
   - **Destination**: 192.168.10.*
   - **Port**: 80
   - **Auto-Detect**: Active
   - **Protocol**: HTTP
   - **Transparent Mode**: Select
   - **Enable Byte Caching**: Select
   - **Enable Secure Tunnel**: Select
   - **Authentication Group**: Auth_Secure_Tunnel
6 Select *OK*.

To configure peers on the server-side FortiGate unit

1 Go to *WAN Opt. & Cache > Peer* and enter a *Local Host ID* for the server-side FortiGate unit:
   - **Local Host ID**: Web_servers
2 Select *Apply* to save your setting.
3 Select *Create New* and add a *Peer Host ID* and the *IP Address* for the client-side FortiGate unit:
   - **Peer Host ID**: User_net
   - **IP Address**: 172.30.120.1
4 Select *OK*. 

---

**Sample Configuration**

```
<table>
<thead>
<tr>
<th>Destination Interface/Zone</th>
<th>port2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>ANY</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

To add the authentication group and WAN optimization rule to the client-side FortiGate unit

1 Go to *Wan Opt. & Cache > Peer > Authentication Group*.
2 Select *Create New* to add a new authentication group to be used for secure tunneling:
   - **Name**: Auth_Secure_Tunnel
   - **Authentication Method**: Pre-shared key
   - **Password**: 2345678
   - **Peer Acceptance**: Accept Any Peer
3 Select *OK*.
4 Go to *Wan Opt. & Cache > Rule*.
5 Select *Create New* to add an active rule that enables secure tunneling and includes the authentication group:
   - **Mode**: Full Optimization
   - **Source**: 172.20.120.[100-200]
   - **Destination**: 192.168.10.*
   - **Port**: 80
   - **Auto-Detect**: Active
   - **Protocol**: HTTP
   - **Transparent Mode**: Select
   - **Enable Byte Caching**: Select
   - **Enable Secure Tunnel**: Select
   - **Authentication Group**: Auth_Secure_Tunnel
6 Select *OK*.

To configure peers on the server-side FortiGate unit

1 Go to *WAN Opt. & Cache > Peer* and enter a *Local Host ID* for the server-side FortiGate unit:
   - **Local Host ID**: Web_servers
2 Select *Apply* to save your setting.
3 Select *Create New* and add a *Peer Host ID* and the *IP Address* for the client-side FortiGate unit:
   - **Peer Host ID**: User_net
   - **IP Address**: 172.30.120.1
4 Select *OK*. 
```
To add the authentication group and WAN optimization rule to the server-side FortiGate unit

2. Select Create New and add a new authentication group to be used for secure tunneling:

   Name: Auth_Secure_Tunnel
   Authentication Method: Pre-shared key
   Password: 2345678
   Peer Acceptance: Accept Any Peer

4. Add the passive rule. The source address matches the 172.20.120.100 to 172.20.120.200 IP address range and the 1-65535 port range. You can also enable web caching for HTTP traffic:

   Mode: Full Optimization
   Source: 172.20.120.100[100-200]
   Destination: 192.168.10.*
   Port: 1-65535
   Auto-Detect: Passive
   Enable Web Cache: Select

5. Select OK.

Configuring WAN optimization with secure tunneling - CLI

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit CLI.

To configure peers on the client-side FortiGate unit and add a firewall policy

1. Add the Local Host ID to the client-side FortiGate configuration:
   
   ```
   config wanopt settings
   set host-id User_net
   end
   ```

2. Add the server-side Local Host ID to the client-side peer list:

   ```
   config wanopt peer
   edit Web_servers
   set ip 192.168.20.1
   end
   ```

3. Add a firewall policy to the server-side FortiGate unit to accept the traffic to be optimized:

   ```
   config firewall policy
   edit 20
   set srcintf port1
   set dstintf port2
   set srcaddr all
   set dstaddr all
   set action accept
   set service ANY
   set schedule always
   ```
To add the authentication group and WAN optimization rule to the client-side FortiGate unit

1. Add a new authentication group to be used for secure tunneling:
   ```
   config wanopt auth-group
   edit Auth_Secure_Tunnel
   set auth-method psk
   set psk 2345678
   end
   ```
   Leave peer-accept at its default value.

2. Add the following active rule to optimize HTTP traffic for IP addresses 172.20.120.100 to 172.20.120.200:
   ```
   config wanopt rule
   edit 1
   set auto-detect active
   set src-ip 172.20.120.100-172.20.120.200
   set dst-ip 192.168.10.0-192.168.10.255
   set port 80
   set proto http
   set secure-tunnel enable
   set auth-group Auth_Secure_Tunnel
   end
   ```
   Leave the rest of the settings at their default values.

To configure peers on the server-side FortiGate unit

1. Add the Local Host ID to the server-side FortiGate configuration:
   ```
   config wanopt settings
   set host-id Web_servers
   end
   ```

2. Add the client-side Local Host ID to the server-side peer list:
   ```
   config wanopt peer
   edit User_net
   set ip 172.20.120.1
   end
   ```

To add the authentication group and WAN optimization rule to the server-side FortiGate unit

1. Add a new authentication group to be used for secure tunneling:
   ```
   config wanopt auth-group
   edit Auth_Secure_Tunnel
   set auth-method psk
   set psk 2345678
   end
   ```
   Leave peer-accept at its default value.

2. Add the following passive rule to the server-side FortiGate unit:
   ```
   config wanopt rule
   edit 5
   set auto-detect passive
   ```
Example: Adding secure tunneling to an active-passive WAN optimization configuration

WAN optimization configuration examples

set src-ip 172.20.120.[100-200]
set dst-ip 192.168.10.0-192.168.10.255
set port 1-65535
set webcache enable
end

Leave status (enable) and mode (full) at their default values.
Web caching

FortiGate WAN optimization web caching is a form of object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. Web caching supports explicit and transparent proxy caching of HTTP 1.0 and HTTP 1.1 web sites. See RFC 2616 for information about web caching for HTTP 1.1. Web caching also supports caching HTTPS sessions provided that you import the correct certificate.

Web caching involves storing HTML pages, images, servlet responses and other web-based objects for later retrieval. FortiGate units cache these objects on a WAN optimization storage location.

There are three significant advantages to using web caching to improve WAN performance:

• reduced WAN bandwidth consumption because fewer requests and responses go over the WAN
• reduced web server load because there are fewer requests for web servers to handle
• reduced latency because responses for cached requests are available from a local FortiGate unit instead of from across the WAN or Internet.

You can use web caching to cache any web traffic that passes through the FortiGate unit, including web pages from web servers on a LAN, WAN or on the Internet. The FortiGate unit caches web objects for all HTTP traffic processed by WAN optimization rules that include web caching.

You can add WAN optimization rules for web caching only. You can also add web caching to WAN optimization rules for HTTP traffic that also include byte caching, protocol optimization, and other WAN optimization features. If you use WAN optimization rules to apply web caching, end users do not have to configure their web browsers to use the FortiGate unit as a proxy server.

**Note:** You can also enable web caching for the FortiGate explicit web proxy. For more information, see “To enable web caching for the explicit web proxy” on page 116.

Web caching cannot determine if a file is compressed (for example a zip file) and caches compressed and non-compressed versions of the same file separately. If the HTTP protocol considers the compressed and uncompressed versions of a file the same object, only the compressed or uncompressed file will be cached.

This chapter contains the following topics:

- Configuring Web Cache Only WAN optimization
- Example: Web Cache Only WAN optimization
- Configuring active-passive web caching
- Example: Active-passive Web Caching
- Configuring peer-to-peer web caching
- Example: Peer-to-peer web caching
- Changing web cache settings
Configuring Web Cache Only WAN optimization

You can use Web Cache Only WAN optimization to cache web pages from any web server. In a Web Cache Only configuration, only one FortiGate unit is involved. All traffic between a client network and one or more web servers is intercepted by a Web Cache Only WAN optimization rule. This rule causes the FortiGate unit to cache pages from the web servers on the FortiGate unit and makes the cached pages available to users on the client network.

You can apply Web Cache Only WAN optimization in two configurations.

In the first configuration, the FortiGate unit caches pages for users on a client network. The FortiGate unit is installed between the client network and the WAN or Internet, and the web server or servers are located elsewhere on the WAN or Internet. See “Example: Web Cache Only WAN optimization” on page 64 for an example of this configuration.

You can also create a reverse proxy web caching configuration where the FortiGate unit is dedicated to providing web caching for a single web server or server farm. In this second configuration, the FortiGate unit is installed between the server network and the WAN or Internet, and users are located elsewhere on the WAN or Internet. See “Example: SSL offloading and reverse proxy web caching for an Internet web server” on page 106 for an example of this configuration.

To enable Web Cache Only, you need to go to WAN Opt. & Cache > Rule and select Create New to add a WAN optimization rule. You then set the Mode to Web Cache Only. If you select this mode, the WAN optimization rule does not perform byte caching or protocol optimization.

WAN optimization rule order affects Web Cache Only rules in the same way as other WAN optimization rules. For more information, see “How list order affects rule matching” on page 40 and “Moving a rule to a different position in the rule list” on page 41.

Note: Since only one FortiGate unit is involved in a Web Cache Only configuration, you do not need to change the WAN optimization peer configuration.

Example: Web Cache Only WAN optimization

This example describes how to configure web caching for users in a client network connecting to a web server network across a WAN.

Network topology and assumptions

This example includes a client network with subnet address 172.20.120.0 connecting to web servers on a network with subnet address 192.168.10.0. Only the communication between the client network and the web server network using Port 80 is to be cached, so the Web Cache Only WAN optimization rule includes the IP addresses of the networks and the Port is set to 80. As well, the firewall policy used in this example includes the addresses of the client and server subnets instead of more general firewall addresses.
General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Add firewall addresses and a firewall policy that accepts traffic to be optimized to the FortiGate unit.

2. Add a Web Cache Only WAN optimization rule to the FortiGate unit.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

Configuring Web Cache Only WAN optimization - web-based manager

Use the following steps to configure the example WAN optimization configuration from the FortiGate unit web-based manager. (CLI steps follow.)

To add the firewall addresses and firewall policy

1. Go to Firewall > Policy > Address and select Create New to add the firewall address for the client network:

   - Address Name: Client_Net
   - Type: Subnet/IP Range
   - Subnet / IP Range: 172.20.120.*
   - Interface: Any

2. Add the firewall address for the web server network:
Example: Web Cache Only WAN optimization

Web caching

1. Go to Firewall > Policy and select Create New to add a firewall policy that accepts traffic to be web cached:

- **Source Interface/Zone**: port1
- **Source Address**: Client_Net
- **Destination Interface/Zone**: port2
- **Destination Address**: Web_Server_Net
- **Schedule**: always
- **Service**: HTTP
- **Action**: ACCEPT

2. Select Web Cache Only.

3. Configure the Web Cache Only rule:

   - **Mode**: Web Cache Only
   - **Source**: 172.20.120.*
   - **Destination**: 192.168.10.*
   - **Port**: 80

   **Tip:** Usually you would set the port to 80 to cache normal HTTP traffic. But you can change the Port to a different number (for example 8080) or to a port number range so that the FortiGate unit provides web caching for HTTP traffic using other ports.

   - **Transparent Mode**: Select
   - **Enable SSL**: Do not select.

   **Tip:** In this example SSL offloading is disabled. For an example of a reverse proxy Web Cache Only configuration that also includes SSL offloading, see "Example: SSL offloading for a WAN optimization tunnel" on page 103.

4. Select OK.

   The rule is added to the bottom of the WAN optimization list.

5. If required, use the Move To icon to move the rule to a different position in the list.

   The order of the rules in the list significantly affects how the rules are applied. For more information, see "How list order affects rule matching" on page 40 and "Moving a rule to a different position in the rule list" on page 41.
Configuring Web Cache Only WAN optimization - CLI

Use the following steps to configure the example WAN optimization configuration from the FortiGate unit CLI.

To add the firewall addresses and firewall policy

1. Add the firewall address for the client network:
   ```
   config firewall address
   edit Client_Net
   set type iprange
   set start-ip 172.20.120.0
   set end-ip 172.20.120.255
   end
   ```

2. Add the firewall address for the web server network:
   ```
   config firewall address
   edit Web_Server_Net
   set type iprange
   set start-ip 192.168.10.0
   set end-ip 192.168.10.255
   end
   ```

3. Add a firewall policy that accepts traffic to be web cached:
   ```
   config firewall policy
   edit 2
   set srcintf port1
   set dstintf port2
   set srcaddr Client_Net
   set dstaddr Web_Server_Net
   set action accept
   set service HTTP
   set schedule always
   end
   ```

To add a Web Cache Only WAN optimization rule

1. Add the following Web Cache Only rule:
   ```
   config wanopt rule
   edit 2
   set mode webcache-only
   set src-ip 172.20.120.0-172.20.120.255
   set dst-ip 192.168.10.0-192.168.10.255
   set port 80
   set peer Peer_Fgt_2
   end
   ```

Accept default settings for transparent (enable), status (enable), ssl (disable), unknown-http-version (tunnel), and tunnel-non-http (disable).

Tip: In this example, SSL offloading is disabled. For an example of a reverse proxy Web Cache Only configuration that also includes SSL offloading, see "Example: SSL offloading for a WAN optimization tunnel" on page 103.
If required, use the `move` command to move the rule to a different position in the list. The order of the rules in the list significantly affects how the rules are applied. For more information, see “How list order affects rule matching” on page 40 and “Moving a rule to a different position in the rule list” on page 41.

**Configuring active-passive web caching**

You add web caching support to the passive or server side of an active-passive WAN optimization configuration. Web pages are cached on the server-side FortiGate unit so you should also select `Enable Byte Caching` for optimum WAN optimization performance.

For web caching to work, the WAN optimization tunnel must accept HTTP (and optionally HTTPS) traffic. To do this, the active rule on the client side must include the ports used for HTTP (and HTTPS) traffic. Set `Protocol` to `HTTP` to perform protocol optimization of the HTTP traffic. You can also enable SSL offloading and secure tunneling, as well as add an authentication group.

**Example: Active-passive Web Caching**

This example describes how to configure active-passive web caching for users in a client network connecting to a web server network across a WAN.

**Network topology and assumptions**

This example configuration includes a client-side FortiGate unit called Client_Side with a WAN IP address of 172.10.10.1 in front of a user network with IP address 172.20.120.0. The server-side FortiGate unit is called Server_Side and has a WAN IP address of 172.20.20.1. This server-side unit is in front of a web server network with IP address 192.168.10.0. Web caching is enabled on the server-side FortiGate unit.
General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the client-side FortiGate unit by adding peers, a firewall policy that accepts traffic to be optimized, and an active WAN optimization rule.

2. Configure the server-side FortiGate unit by adding peers and a passive WAN optimization rule that includes web caching.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

Configuring active-passive web caching - web-based manager

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit web-based manager. (CLI steps follow.)

To configure the client-side FortiGate unit

1. Go to WAN Opt. & Cache > Peer and enter a Local Host ID for the client FortiGate unit:
   - Local Host ID: Client_Side

2. Select Apply to save your setting.

3. Select Create New and add a Peer Host ID and the IP Address for the server-side FortiGate unit:
   - Peer Host ID: Server_Side
   - IP Address: 172.20.20.1
4  Select OK.
5  Go to Firewall > Policy and add a firewall policy that accepts traffic to be web cached:

- Source Interface/Zone: port1
- Source Address: all
- Destination Interface/Zone: port2
- Destination Address: all
- Schedule: always
- Service: ANY
- Action: ACCEPT

6  Go to WAN Opt. & Cache > Rule and select Create New.
7  Configure the rule:

- Mode: Full Optimization
- Source: 172.20.120.*
- Destination: 192.168.10.*
- Port: 1-65535
- Auto-Detect: Active
- Protocol: HTTP
- Transparent Mode: Select
- Enable Byte Caching: Select

8  Select OK.
   The rule is added to the bottom of the WAN optimization list.
9  If required, use the Move To icon to move the rule to a different position in the list.
   The order of the rules in the list significantly affects how the rules are applied. For more information, see “How list order affects rule matching” on page 40 and “Moving a rule to a different position in the rule list” on page 41.

To configure the server-side FortiGate unit
1  Go to WAN Opt. & Cache > Peer and enter a Local Host ID for the server-side FortiGate unit:
   Local Host ID: Server_Side
2  Select Apply to save your setting.
3  Select Create New and add a Peer Host ID and the IP Address for the client-side FortiGate unit:
   Peer Host ID: Client_Side
   IP Address: 172.10.10.1

4  Go to WAN Opt. & Cache > Rule and select Create New.
5  Configure the passive web cache rule:

- Mode: Full Optimization
- Source: 172.20.120.*
The rule is added to the bottom of the WAN optimization rule list.

7 If required, use the Move To icon to move the rule to a different position in the list.
For more information, see “Moving a rule to a different position in the rule list” on page 41.

Configuring active-passive web caching - CLI

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit CLI.

To configure the client-side FortiGate unit

1 Add the Local Host ID to the client-side FortiGate configuration:
   ```
   config wanopt settings
   set host-id Client_Side
   end
   ```

2 Add the server-side Local Host ID to the client-side peer list:
   ```
   config wanopt peer
   edit Server_Side
   set ip 172.20.20.1
   end
   ```

3 Add a firewall policy to the server-side FortiGate unit to accept the traffic to be optimized:
   ```
   config firewall policy
   edit 23
   set srcintf port1
   set dstintf port2
   set srcaddr all
   set dstaddr all
   set action accept
   set service ANY
   set schedule always
   end
   ```

4 Configure the following active rule:
   ```
   config wanopt rule
   edit 2
   set auto-detect active
   set src-ip 172.20.120.0-172.20.120.255
   set dst-ip 192.168.10.0-192.168.10.255
   set port 1-65535
   set proto http
   ```
Accept default settings for transparent (enable), status (enable), mode (full), byte-caching (enable), ssl (disable), secure-tunnel (disable), auth-group (null), unknown-http-version (tunnel), and tunnel-non-http (disable).

5 If required, use the move command to move the rule to a different position in the list.

The order of the rules in the list significantly affects how the rules are applied. For more information, see “How list order affects rule matching” on page 40 and “Moving a rule to a different position in the rule list” on page 41.

To configure the server-side FortiGate unit

1 Add the Local Host ID to the server-side FortiGate configuration:
   
   config wanopt settings
   set host-id Server_Side
   end

2 Add the client-side Local Host ID to the server-side peer list:

   config wanopt peer
   edit Client_Side
   set ip 172.10.10.1
   end

3 Add the following passive web cache rule:

   config wanopt rule
   edit 5
   set auto-detect passive
   set src-ip 172.20.120.0-172.20.120.255
   set dst-ip 192.168.10.0-192.168.10.255
   set port 1-65535
   set webcache enable
   end

   Accept default settings for status (enable) and mode (full).

4 If required, use the move command to move the rule to a different position in the list so that the tunnel request from the client-side FortiGate unit matches with this rule.

For more information, see “Moving a rule to a different position in the rule list” on page 41.

Configuring peer-to-peer web caching

In a peer-to-peer web caching configuration, you create a peer-to-peer WAN optimization rule on the client-side FortiGate unit and include the peer host ID of the server-side FortiGate unit. In the rule, you set Auto-Detect to Off and select Enable Web Cache. Using this rule, the client-side FortiGate unit can create a WAN optimization tunnel only with the peer that is added to the rule.

In a peer-to-peer configuration, you do not have to add a rule to the server-side FortiGate unit. If the server-side FortiGate unit peer list contains the client FortiGate unit, the server FortiGate unit accepts WAN optimization tunnel connections from the client FortiGate unit and the two units can form a WAN optimization tunnel. The server-side FortiGate unit uses the settings in the rule added to the client-side FortiGate unit.
For web caching to work, the WAN optimization tunnel must allow HTTP (and optionally HTTPS) traffic. To do this, the WAN optimization rule must include the ports used for HTTP (and HTTPS) traffic. Set Protocol to HTTP to perform protocol optimization of the HTTP traffic. You can also enable WAN optimization transparent mode, byte caching, SSL offloading, and secure tunneling, as well as add an authentication group.

**Example: Peer-to-peer web caching**

This example describes how to configure peer-to-peer web caching for users in a client network connecting to a web server network across a WAN.

### Network topology and assumptions

This example configuration includes a client-side FortiGate unit called Client_Side with a WAN IP address of 172.10.10.1 in front of a user network with IP address 172.20.120.0. The server-side FortiGate unit is called Server_Side and has a WAN IP address of 172.20.20.1. This server-side unit is in front of a web server network with IP address 192.168.10.0. Web caching is enabled on the server-side FortiGate unit.
Figure 37: Example peer-to-peer web cache topology

General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the client-side FortiGate unit by adding peers, a firewall policy that accepts traffic to be optimized, and a peer-to-peer WAN optimization rule that includes web caching.

2. Configure the server-side FortiGate unit.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

Configuring peer-to-peer web caching - web-based manager

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit web-based manager. (CLI steps follow.)

To configure the client-side FortiGate unit

1. Go to WAN Opt. & Cache > Peer and enter a Local Host ID for the client FortiGate unit:

   Local Host ID: Client_Side

2. Select Apply to save your setting.

3. Select Create New and add a Peer Host ID and the IP Address for the server-side FortiGate unit:

   Peer Host ID: Server_Side
   IP Address: 192.168.30.12

4. Select OK.

5. Go to Firewall > Policy and add a firewall policy that accepts traffic to be web cached:

   Source Interface/Zone: port1
   Source Address: all
   Destination Interface/Zone: port2
   Destination Address: all
Web caching

Example: Peer-to-peer web caching

6 Go to WAN Opt. & Cache > Rule and select Create New.

7 Configure the rule:

- **Schedule**: always
- **Service**: ANY
- **Action**: ACCEPT

8 Select OK.

The rule is added to the bottom of the WAN optimization list.

9 If required, use the Move To icon to move the rule to a different position in the list.

The order of the rules in the list significantly affects how the rules are applied. For more information, see “How list order affects rule matching” on page 40 and “Moving a rule to a different position in the rule list” on page 41.

Figure 38: Adding the client-side peer host ID to the server-side peer list

<table>
<thead>
<tr>
<th>New WAN Optimization Peer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer Host ID</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>172.40.120.100</td>
</tr>
</tbody>
</table>

**To configure the server-side FortiGate unit**

1 Go to WAN Opt. & Cache > Peer and enter a **Local Host ID** for the server FortiGate unit:

- **Local Host ID**: Server_Side

2 Select **Apply** to save your setting.

3 Select **Create New** and add a **Peer Host ID** and the **IP Address** for the client-side FortiGate unit:

- **Peer Host ID**: Client_Side
- **IP Address**: 172.20.34.12

4 Select **OK**.
Configuring peer-to-peer web caching - CLI

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit CLI.

To configure the client-side FortiGate unit

1. Add the Local Host ID to the client-side FortiGate configuration:
   ```
   config wanopt settings
   set host-id Client_Side
   end
   ```

2. Add the server-side Local Host ID to the client-side peer list:
   ```
   config wanopt peer
   edit Server_Side
   set ip 192.168.30.12
   end
   ```

3. Add a firewall policy to the server-side FortiGate unit to accept the traffic to be optimized:
   ```
   config firewall policy
   edit 23
   set srcintf port1
   set dstintf port2
   set srcaddr all
   set dstaddr all
   set action accept
   set service ANY
   set schedule always
   end
   ```

4. Configure the following active rule:
   ```
   config wanopt rule
   edit 5
   set auto-detect off
   set src-ip 172.20.120.*
   set dst-ip 192.168.10.*
   set port 80
   set proto http
   set peer Server_Side
   set web cache enable
   ```

   Accept default settings for transparent (enable), status (enable), mode (full), byte-caching (enable), ssl (disable), secure-tunnel (disable), auth-group (null), unknown-http-version (tunnel), and tunnel-non-http (disable).

5. If required, use the move command to the rule to a different position in the list.

   The order of the rules in the list significantly affects how the rules are applied. For more information, see “How list order affects rule matching” on page 40 and “Moving a rule to a different position in the rule list” on page 41.

To configure the server-side FortiGate unit

1. Add the Local Host ID to the server-side FortiGate configuration:
   ```
   config wanopt settings
   ```
Changing web cache settings

In most cases, the default settings for the WAN optimization web cache are acceptable. However, you may want to change them to improve performance or optimize the cache for your configuration. To change these settings, go to WAN Opt. & Cache > Cache.

From the FortiGate CLI, you can use the `config wanopt webcache` command to change these WAN optimization web cache settings. For more information, see the FortiGate CLI Reference.

**Note:** For more information about many of these web cache settings, see RFC 2616.

### Figure 39: Web Cache Settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Options</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always Revalidate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max Cache Object Size</td>
<td></td>
<td>512000 KB</td>
</tr>
<tr>
<td>Negative Response Duration</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Fresh Factor</td>
<td></td>
<td>100</td>
</tr>
<tr>
<td>Max TTL</td>
<td></td>
<td>72000</td>
</tr>
<tr>
<td>Min TTL</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Default TTL</td>
<td></td>
<td>1440</td>
</tr>
<tr>
<td>Explicit Proxy</td>
<td></td>
<td>(enabled)</td>
</tr>
<tr>
<td>Ignore</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If-modified-since</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP 1.1 Conditionals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pragma-no-cache</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IE Reload</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cache Expired Objects</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revalidated Pragma-no-cache</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Always revalidate**
Select to always revalidate requested cached objects with content on the server before serving them to the client.

**Max Cache Object Size**
Set the maximum size of objects (files) that are cached. The default size is 512000 KB. This setting determines the maximum object size to store in the web cache. Objects that are larger than this size are still delivered to the client but are not stored in the FortiGate web cache.

**Negative Response Duration**
Set how long in minutes to cache negative responses. The default is 0, meaning negative responses are not cached. The content server might send a client error code (4xx HTTP response) or a server error code (5xx HTTP response) as a response to some requests. If the web cache is configured to cache these negative responses, it returns that response in subsequent requests for that page or image for the specified number of minutes.
**Fresh Factor**
Set the fresh factor as a percentage. The default is 100, and the range is 1 to 100. For cached objects that do not have an expiry time, the web cache periodically checks the server to see if the objects have expired. The higher the Fresh Factor the less often the checks occur.

For example, if you set the Max TTL value and Default TTL to 7200 minutes (5 days) and set the Fresh Factor to 20, the web cache check the cached objects 5 times before they expire, but if you set the Fresh Factor to 100, the web cache will check once.

**Max TTL**
The maximum amount of time (Time to Live) an object can stay in the web cache without the cache checking to see if it has expired on the server. The default is 7200 minutes (120 hours or 5 days).

**Min TTL**
The minimum amount of time an object can stay in the web cache before the web cache checks to see if it has expired on the server. The default is 5 minutes.

**Default TTL**
The default expiry time for objects that do not have an expiry time set by the web server. The default expiry time is 1440 minutes (24 hours).

**Explicit Proxy**
Indicates whether the explicit web proxy has been enabled for the FortiGate unit. See "Configuring the explicit web proxy" on page 164.

**Enable Cache Explicit Proxy**
Select to use WAN optimization web caching to cache content received by the explicit web proxy.

**Ignore**

- **If-modified-since**
  By default, if the time specified by the if-modified-since (IMS) header in the client's conditional request is greater than the last modified time of the object in the cache, it is a strong indication that the copy in the cache is stale. If so, HTTP does a conditional GET to the Overlay Caching Scheme (OCS), based on the last modified time of the cached object.
  Enable ignoring if-modified-since to override this behavior.

- **HTTP 1.1 Conditionals**
  HTTP 1.1 provides additional controls to the client over the behavior of caches toward stale objects. Depending on various cache-control headers, the FortiGate unit can be forced to consult the OCS before serving the object from the cache. For more information about the behavior of cache-control header values, see RFC 2616.

- **Pragma-no-cache**
  Typically, if a client sends an HTTP GET request with a pragma no-cache (PNC) or cache-control no-cache header, a cache must consult the OCS before serving the object from the cache. This means that the FortiGate unit always re-fetches the entire object from the OCS, even if the cached copy of the object is fresh.
  Because of this behavior, PNC requests can degrade performance and increase server-side bandwidth utilization. However, if you enable ignoring Pragma-no-cache, then the PNC header from the client request is ignored. The FortiGate unit treats the request as if the PNC header is not present.

- **IE Reload**
  Some versions of Internet Explorer issue Accept / header instead of Pragma no-cache header when you select Refresh. When an Accept header has only the / value, the FortiGate unit treats it as a PNC header if it is a type-N object.
  Enable ignoring IE reload to cause the FortiGate unit to ignore the PNC interpretation of the Accept / header.
Cache Expired Objects

- Applies only to type-1 objects. When this option is selected, expired type-1 objects are cached (if all other conditions make the object cacheable).

Revalidated Pragma-no-cache

- The pragma-no-cache (PNC) header in a client's request can affect how efficiently the FortiGate unit uses bandwidth. If you do not want to completely ignore PNC in client requests (which you can do by selecting to ignore Pragma-no-cache, above), you can nonetheless lower the impact on bandwidth usage by selecting Revalidate Pragma-no-cache.

  When you select Revalidate Pragma-no-cache, a client's non-conditional PNC-GET request results in a conditional GET request sent to the OCS if the object is already in the cache. This gives the OCS a chance to return the 304 Not Modified response, which consumes less server-side bandwidth, because the OCS has not been forced to otherwise return full content.

  By default, Revalidate Pragma-no-cache is disabled and is not affected by changes in the top-level profile.

  Most download managers make byte-range requests with a PNC header. To serve such requests from the cache, you should also configure byte-range support when you configure the Revalidate pragma-no-cache option.
Advanced configuration example

This chapter contains an advanced WAN optimization configuration example that combines many of the concepts described in the previous chapters of this document. The configuration example described here includes active-passive rules, web caching, policy routes for out-of-path WAN optimization, and multiple VDOMs with inter-VDOM routing to apply protection profiles to traffic before it is optimized.

Out-of-path WAN optimization with inter-VDOM routing

This example describes how to configure out-of-path WAN optimization to optimize web browsing and FTP file transfers between a client network and a server network.

Network topology and assumptions

The client network connects to the Internet through a FortiGate-300A unit, and the server network connects to the Internet through a cluster of two FortiGate-1000A units.

Adding in-path WAN optimization requires replacing these FortiGate units with models that support WAN optimization or adding new FortiGate units in the data path. In either of these in-path configurations, the optimizing FortiGate units would also be required to support all traffic on the data path plus provide WAN optimization.

The out-of-path topology shown in Figure 40 offloads WAN optimization to out-of-path FortiGate units that only process sessions to be optimized. The topology includes a FortiGate-311B unit installed at the client network and a single FortiGate-620B unit installed at the server network.

Note: The FortiGate-620B unit is installed at the server network because other client networks also use it for WAN optimization. The configuration for those other client networks is not described in this example.

Figure 40: Out-of-path WAN optimization
The client-side FortiGate-300A unit uses policy routing to offload WAN optimization of HTTP and FTP sessions by re-directing all HTTP and FTP sessions to the FortiGate-311B unit. The FortiGate-311B and 620B units work together to apply web caching, byte caching, and HTTP and FTP protocol optimization to HTTP and FTP sessions. The WAN optimization tunnel between the 311B and the 620B operates in Transparent mode. The FortiGate-311B unit also web caches all Internet HTTP traffic from the client network.

The client-side FortiGate-311B unit also applies a protection profile to the HTTP and FTP traffic. To do this, the FortiGate-311B unit is configured for multiple VDOM operation. A new VDOM named Wanopt is added to the FortiGate-311B. HTTP and FTP sessions are received by the “root” VDOM. Firewall policies in the root VDOM accept HTTP and FTP sessions and apply a protection profile to them. To preserve the source addresses of the HTTP and FTP sessions, NAT is not enabled for these policies.

The sessions are then routed through an inter-VDOM link to the Wanopt VDOM. The Wanopt VDOM includes firewall policies that accept the HTTP and FTP sessions and WAN optimization rules that apply WAN optimization and web caching to the sessions.

The server-side FortiGate-620B unit includes a passive WAN optimization rule that accepts WAN optimization tunnel requests from the FortiGate-311B unit. Only one passive rule is required on the FortiGate-620B unit. The FortiGate-620B unit also forwards sessions to the server-side FortiGate-1000A cluster which forwards them to the server network.

WAN optimization is operating in Transparent mode, so the packets from the client network include their client network source IP addresses. To preserve these source IP addresses, the firewall policies on the FortiGate-1000A cluster that accept the sessions from the FortiGate-620B unit should not apply NAT. If the firewall policies were to apply NAT, the client network addresses would be replaced with the port1 IP address of the FortiGate-1000A cluster and the client network source IP addresses would be lost.

The optimizing FortiGate units operate in NAT/Route mode and are directly connected to the Internet. This configuration requires two Internet connections and two Internet IP addresses for each network. (Reminder: All of the example IP addresses shown in Figure 40 are private IP addresses because all Fortinet documentation examples use only private IP addresses.) If these extra Internet IP addresses are not available, you can install a router between the WAN and the FortiGate units or install the optimizing FortiGate units out of path on the private networks and configure routing on the private networks to route HTTP and FTP sessions to the optimizing FortiGate units.

**Configuration steps**

This example is divided into client-side and the server-side steps, as configured through the web-based manager and the CLI. Use either method, but for best results, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

This example includes the following sections:

- “Client-side configuration steps - web-based manager” on page 83
- “Server-side configuration steps - web-based manager” on page 90
- “Client-side configuration steps - CLI” on page 93
- “Server-side configuration steps - CLI” on page 100
Client-side configuration steps - web-based manager

This section describes the configuration steps required to redirect HTTP and FTP sessions from the client-side FortiGate-300A unit and to configure the client-side FortiGate-311B unit to optimize HTTP and FTP sessions to the server network and to apply web caching to all other HTTP sessions from the client network.

The section breaks down the client-side configuration into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the FortiGate-300A unit to redirect all HTTP and FTP sessions to the FortiGate-311B unit.
2. Configure the FortiGate-311B unit for multiple VDOM operation and add an inter-VDOM link.
3. Configure routing for the FortiGate-311B root VDOM.
4. Add firewall policies to the FortiGate-311B root VDOM to accept HTTP and FTP sessions received at port1 and destined for Vlink0, and apply a protection profile.
5. Configure routing for the FortiGate-311B Wanopt VDOM.
6. Add firewall policies to the FortiGate-311B Wanopt VDOM to accept HTTP and FTP sessions received at the Vlink1 interface of the inter-VDOM link and destined for port10.
7. Configure peers for the FortiGate-311B Wanopt VDOM.
8. Add WAN optimization rules for HTTP and FTP to the FortiGate-311B Wanopt VDOM.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

To configure the FortiGate-300A unit to redirect all HTTP and FTP sessions to the FortiGate-311B unit

1. Go to System > Network > Interface, edit port4, and set the port4 IP address to 172.10.10.1/24.
2. Go to Firewall > Policy and select Create New to add a firewall policy that allows all port5 to port4 HTTP sessions:

   - Source Interface/Zone: port5
   - Source Address: all
   - Destination Interface/Zone: port4
   - Destination Address: all
   - Schedule: always
   - Service: HTTP
   - Action: ACCEPT
   - NAT: Select

   Configure other policy settings that you may require. For example, you could add a protection profile.
3. Select Create New to add a firewall policy that allows all port5 to port4 FTP sessions:
Configure other policy settings that you may require.

4 Select OK.

5 If required, use the Move To icon to change the order of the firewall policies. Follow the normal rules for ordering firewall policies in the policy list. For example, move specific rules above general rules. For more information about these rules, see the FortiGate Administration Guide.

6 Go to Router > Static > Policy Route and select Create New to add a policy route to redirect HTTP traffic received at port5 to exit the FortiGate unit using port4. Set the gateway address of the route to 172.10.10.2 so that the HTTP sessions are directed to the FortiGate-311B port1 interface. For HTTP traffic, the protocol is 6 (TCP) and the destination port is 80:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port4</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>FTP</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>NAT</td>
<td>Select</td>
</tr>
</tbody>
</table>

7 Select OK.

8 Select Create New to add a policy route to redirect FTP traffic received at port5 to exit the FortiGate unit using port4. Set the gateway address of the route to 172.10.10.2 so that the HTTP sessions are directed to the FortiGate-311B port1 interface. For FTP traffic, the protocol is 6 (TCP) and the destination port is 21:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming interface</td>
<td>port5</td>
</tr>
<tr>
<td>Source address / mask</td>
<td>0.0.0.0/0.0.0.0</td>
</tr>
<tr>
<td>Destination address / mask</td>
<td>0.0.0.0/0.0.0.0</td>
</tr>
<tr>
<td>Destination Ports</td>
<td>From 80 to 80</td>
</tr>
<tr>
<td>Type of Service</td>
<td>bit pattern: 00 (hex) bit mask: 00 (hex)</td>
</tr>
<tr>
<td>Outgoing interface</td>
<td>port4</td>
</tr>
<tr>
<td>Gateway Address</td>
<td>172.10.10.2</td>
</tr>
</tbody>
</table>

9 Select OK.
To configure the FortiGate-311B unit for multiple VDOM operation and add an inter-VDOM link

1. Go to System > Status > Dashboard.
2. In the System Information widget, select Enable beside Virtual Domain to enable multiple VDOM operation and log back in to the web-based manager.
3. Go to System > VDOM and select Create New to add a new virtual domain named Wanopt.
4. Select OK twice to add the Wanopt VDOM with default resource limits.
5. Go to System > Network, edit the port10 interface, and configure the following settings to add the port10 interface to the Wanopt VDOM:

   **Virtual Domain**: Wanopt  
   **Addressing Mode**: Manual  
   **IP/Netmask**: 10.10.10.2/24

   Configure other settings that you may require.
6. Select OK.
7. Select Create New > VDOM Link and add an inter-VDOM link with the following settings:

   **Name**: Vlink
   **Interface #0**
   - **Virtual Domain**: root
   - **IP/Netmask**: 172.1.1.1/24
   **Interface #1**
   - **Virtual Domain**: Wanopt
   - **IP/Netmask**: 172.1.1.2/24

8. Select OK.

To configure routing for the FortiGate-311B root VDOM

1. Log in to the root VDOM.
2. Go to Router > Static and select Create New to add a default route. The destination of the default route is the inter-VDOM link interface in the root VDOM. The gateway of the default route is the IP address of the inter-VDOM link interface in the Wanopt VDOM. The result is the default route sends all traffic out the inter-VDOM link and into the Wanopt VDOM:

   **Destination IP/Mask**: 0.0.0.0/0.0.0.0
   **Device**: Vlink0
   **Gateway**: 172.1.1.2
   **Distance**: 10

3. Select OK.
4. Select Create New to add a route to send return traffic from the server network destined for the client network out the port1 interface to the port4 interface of the FortiGate-300A which has IP address 172.10.10.1:
To add firewall policies to the FortiGate-311B root VDOM to accept HTTP and FTP sessions received at port1 destined for Vlink0 and apply a protection profile:

1. Log in to the root VDOM.

2. Go to `Firewall > Policy` and select `Create New` to add a firewall policy that accepts HTTP sessions received at port1 destined for Vlink0 and applies a protection profile to them:

   | Source Interface/Zone | port1 |
   | Source Address       | all   |
   | Destination Interface/Zone | Vlink0 |
   | Destination Address  | all   |
   | Schedule             | always|
   | Service              | HTTP  |
   | Action               | ACCEPT|
   | NAT                  | Do not select. |

   **Tip:** To preserve the source addresses of the HTTP sessions, NAT should not be enabled for this policy.

   | Protection Profile | scan (Alternatively, you can create a custom protection profile) |

Configure other policy settings that you may require. You can also use more specific firewall addresses or add one firewall policy that accepts both FTP and HTTP traffic.

3. Select OK.

4. Go to `Firewall > Policy` and select `Create New` to add a firewall policy that accepts FTP sessions received at port1 and destined for Vlink0 and applies a protection profile to them:

   | Source Interface/Zone | port1 |
   | Source Address       | all   |
   | Destination Interface/Zone | Vlink0 |
   | Destination Address  | all   |
   | Schedule             | always|
   | Service              | FTP   |
   | Action               | ACCEPT|
   | NAT                  | Do not select. |

   **Tip:** To preserve the source addresses of the FTP sessions, NAT should not be enabled for this policy.

   | Protection Profile | scan (Alternatively, you can instead create a custom protection profile.) |

Configure other policy settings that you may require. You can also use more specific firewall addresses or add one firewall policy that accepts both FTP and HTTP traffic.
5 Select OK.

**To configure routing for the FortiGate-311B Wanopt VDOM**

1 Log in to the Wanopt VDOM.

2 Go to *Router > Static* and select *Create New* to add a default route. The destination of the default route is the port10 interface. The gateway of the default route is the next hop router that the port10 interface connects with:

<table>
<thead>
<tr>
<th>Destination IP/Mask</th>
<th>0.0.0.0/0.0.0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>port10</td>
</tr>
<tr>
<td>Gateway</td>
<td>(next hop router IP address)</td>
</tr>
<tr>
<td>Distance</td>
<td>10</td>
</tr>
</tbody>
</table>

3 Select OK.

4 Select *Create New* to add a route to send return traffic from the server network destined for the client network out the Vlink1 interface to the Vlink0 interface in the root VDOM, which has the IP address 172.1.1.2:

<table>
<thead>
<tr>
<th>Destination IP/Mask</th>
<th>172.20.120.0/24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Vlink1</td>
</tr>
<tr>
<td>Gateway</td>
<td>172.1.1.2</td>
</tr>
<tr>
<td>Distance</td>
<td>10</td>
</tr>
</tbody>
</table>

5 Select OK.

**To add firewall policies to the FortiGate-311B Wanopt VDOM to accept HTTP and FTP sessions received at the Vlink1 interface of the inter-VDOM link and destined for port10**

1 Log in to the Wanopt VDOM.

2 Go to *Firewall > Policy* and select *Create New* to add a firewall policy that accepts HTTP sessions received at Vlink1 and destined for port10:
Configure other settings that you may require.

3 Select OK.

4 Go to Firewall > Policy and select Create New to add a firewall policy that accepts FTP sessions received at Vlink1 and destined for port10:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Vlink1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port10</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>FTP</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>NAT</td>
<td>Select</td>
</tr>
</tbody>
</table>

**Tip:** NAT is ignored for all FTP sessions for the server network because these sessions are intercepted by a full optimization WAN optimization rule. However, FTP sessions for the Internet are allowed to reach their destination, so source NAT is required for replies.

**Protection Profile**

- Do not select.

**Tip:** Do not select a protection profile because you cannot apply a protection profile and WAN optimization to the same session in the same VDOM. A protection profile was applied to the session in the root VDOM.

Configure other settings that you may require.

5 Select OK.

To configure peers for the FortiGate-311B Wanopt VDOM

1 Log in to the Wanopt VDOM.
2 Go to WAN Opt. & Cache > Peer and enter a Local Host ID for the client-side FortiGate-311B unit:

   Local Host ID       Client_Fgt

3 Select Apply to save your setting.

4 Select Create New and add a Peer Host ID and the IP Address for the server-side FortiGate-620B unit:

   Peer Host ID       Server_Fgt
   IP Address         10.20.20.2

5 Select OK.

To add WAN optimization rules for HTTP and FTP to the FortiGate-311B Wanopt VDOM

1 Log in to the Wanopt VDOM.

2 Go to WAN Opt. & Cache > Rule.

3 Select Create New to add an active rule to optimize HTTP traffic from IP addresses on the Client network (172.20.120.0) with a destination address on the server network (192.168.10.0):

   Mode              Full Optimization
   Source            172.20.120.*
   Destination       192.168.10.*
   Port              80
   Auto-Detect       Active
   Protocol          HTTP
   Transparent Mode  Select
   Enable Byte Caching Select
   Enable SSL        Do not select.
   Enable Secure Tunnel Do not select.

   Tip: For improved privacy you can select this option and add an authentication group to both optimizing FortiGate units.

   Authentication Group Do not select.

4 Select OK.

5 Select Create New to add an active rule to optimize FTP traffic from IP addresses on the Client network (172.20.120.0) with a destination address on the server network (192.168.10.0):

   Mode              Full Optimization
   Source            172.20.120.*
   Destination       192.168.10.*
   Port              21
   Auto-Detect       Active
   Protocol          FTP
   Transparent Mode  Select
   Enable Byte Caching Select
Out-of-path WAN optimization with inter-VDOM routing

Advanced configuration example

Enable SSL: Do not select.
Enable Secure Tunnel: Do not select.

**Tip:** For improved privacy you can select this option and add an authentication group to both optimizing FortiGate units.

Authentication Group: Do not select.

6 Select OK.

7 Select Create New to add a rule to web cache HTTP traffic from IP addresses on the Client network (172.20.120.0) with any destination address:

- **Mode:** Web Cache Only
- **Source:** 172.20.120.*
- **Destination:** 0.0.0.0
- **Port:** 80
- **Transparent Mode:** Select
- **Enable SSL:** Do not select.

Select OK.

8 If required, use the Move To icon to move the Web Cache Only rule below the full optimization HTTP and FTP rules in the list. The Web Cache Only rule should be below the full optimization rules because it will match all HTTP traffic and you need HTTP sessions with destination address 192.168.10.0 to match the full optimization HTTP rule.

### Server-side configuration steps - web-based manager

This section describes the configuration steps required for the server-side FortiGate-620B unit to perform WAN optimization with the client-side FortiGate-311B unit and to send HTTP and FTP sessions to the server-side FortiGate-1000A cluster. This section also describes how to configure the FortiGate-1000A cluster to forward HTTP and FTP sessions from the client network to the server network.

The section breaks down the client-side configuration into smaller procedures. For best results, follow the procedures in the order given:

1 Configure routing for the FortiGate-620B unit.

2 Configure peers for the server-side FortiGate-620B unit.

3 Add a passive WAN optimization rule to the server-side FortiGate-620B unit.

4 Configure the FortiGate-1000A cluster to accept HTTP and FTP connections at port5 and forward them out port1 to the server network.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

**To configure routing for the FortiGate-620B unit**

1 Go to **Router > Static** and select Create New to add a default route. The destination of the default route is the port16 interface. The gateway of the default route is the next hop router that the port16 interface connects with:

- **Destination IP/Mask:** 0.0.0.0/0.0.0.0
- **Device:** port16
- **Gateway:** (next hop router IP address)
- **Distance:** 10
2 Select OK.

3 Select Create New to add a route to send traffic for the server network out port1 to the port5 interface of the FortiGate-1000A cluster, which has the IP address 192.20.20.1:

- **Destination IP/Mask**: 192.168.10.0/24
- **Device**: port1
- **Gateway**: 192.20.20.1
- **Distance**: 10

4 Select OK.

To configure peers for the server-side FortiGate-620B unit

1 Go to WAN Opt. & Cache > Peer and enter a Local Host ID for the server-side FortiGate-620B unit:

- **Local Host ID**: Server_Fgt

2 Select Apply to save your setting.

3 Select Create New and add a Peer Host ID and the IP Address for the client-side FortiGate-311B unit:

- **Peer Host ID**: Client_Fgt
- **IP Address**: 10.10.10.2

4 Select OK.

To add a passive WAN optimization rule to the server-side FortiGate-620B unit

You can add one passive WAN optimization rule to the server-side FortiGate-620B unit for both active rules on the FortiGate-311B unit. This rule can also allow the FortiGate-620B to perform WAN optimization with other client-side devices as long as the required Peer Host IDs are added to the FortiGate-620B configuration and to the client-side configurations.

1 Go to WAN Opt. & Cache > Rule and select Create New to add a passive rule that accepts any WAN optimization tunnel request:

- **Mode**: Full Optimization
- **Source**: 0.0.0.0
- **Destination**: 192.168.10.*
- **Port**: 1-65535
  - **Tip**: You can also use a narrower port range such as 21-80 or add two rules, one with port set to 80 and one with port set to 21.
- **Auto-Detect**: Passive
- **Enable Web Cache**: Select

2 Select OK.

3 If required, use the Move To icon to move the rule to a different position in the list so that the tunnel request from the client-side FortiGate unit matches with this rule.

For more information, see "Moving a rule to a different position in the rule list" on page 41.
To configure the FortiGate-1000A cluster to accept HTTP and FTP connections at port5 and forward them out port1 to the server network:

1. Go to **Firewall > Address** and select **Create New** to add an address for the server network:
   - **Address Name**: Server_Net
   - **Type**: Subnet / IP Range
   - **Subnet / IP Range**: 192.168.10.*
   - **Interface**: Any
   - Select **OK**.

2. Go to **Firewall > Address** and select **Create New** to add an address for the client network:
   - **Address Name**: Client_Net
   - **Type**: Subnet / IP Range
   - **Subnet / IP Range**: 172.20.120.*
   - **Interface**: Any
   - Select **OK**.

3. Go to **Firewall > Policy** and select **Create New** to add an firewall policy that accepts HTTP sessions at port5 destined for port1 and the server network:
   - **Source Interface/Zone**: port5
   - **Source Address**: Client_Net
   - **Destination Interface/Zone**: port1
   - **Destination Address**: Server_Net
   - **Schedule**: always
   - **Service**: HTTP
   - **Action**: ACCEPT
   - **NAT**: Do not select.
   - **Tip**: WAN optimization is operating in Transparent mode so the packets from the client network include their client network source IP addresses. To preserve these source IP addresses the firewall policies on the FortiGate-1000A cluster that accept the sessions from the FortiGate-620B unit should not apply NAT. If the policies were to apply NAT, the client network addresses would be replaced with the port1 IP address of the FortiGate-1000A cluster and the client network source IP addresses would be lost.
   - Select **OK**.

4. Go to **Firewall > Policy** and select **Create New** to add an firewall policy that accepts FTP sessions at port5 destined for port1 and the server network:
   - **Source Interface/Zone**: port5
   - **Source Address**: Client_Net
   - **Destination Interface/Zone**: port1
   - **Destination Address**: Server_Net
   - **Schedule**: always
   - **Service**: FTP
   - **Action**: ACCEPT
   - **NAT**: Do not select.
Client-side configuration steps - CLI

This section describes the configuration steps required to redirect HTTP and FTP sessions from the client-side FortiGate-300A unit and to configure the client-side FortiGate-311B unit to optimize HTTP and FTP sessions to the server network and to apply web caching to all other HTTP sessions from the client network.

The section breaks down the client-side configuration into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the FortiGate-300A unit to redirect all HTTP and FTP sessions to the FortiGate-311B unit.
2. Configure the FortiGate-311B unit for multiple VDOM operation and add an inter-VDOM link.
3. Configure routing for the FortiGate-311B root VDOM.
4. Add firewall policies to the FortiGate-311B root VDOM to accept HTTP and FTP sessions received at port1 and destined for Vink0, and apply a protection profile.
5. Configure routing for the FortiGate-311B Wanopt VDOM.
6. Add firewall policies to the FortiGate-311B Wanopt VDOM to accept HTTP and FTP sessions received at the Vlink1 interface of the inter-VDOM link and destined for port10.
7. Configure peers for the FortiGate-311B Wanopt VDOM.
8. Add WAN optimization rules for HTTP and FTP to the FortiGate-311B Wanopt VDOM. Also note that if you perform any additional actions between procedures, your configuration may have different results.

To configure the FortiGate-300A unit to redirect all HTTP and FTP sessions to the FortiGate-311B unit

1. Set the FortiGate-300A port4 IP address to 172.10.10.1:
   ```
   config system interface
   edit port4
   set ip 172.10.10.1/24
   end
   ```

2. Add a firewall policy that allows all port5 to port4 HTTP sessions:
   ```
   config firewall policy
   edit 1
   set srcintf port5
   set dstintf port4
   set srcaddr all
   set dstaddr all
   set action accept
   set service HTTP
   set schedule always
   ```

Tip: As described above, selecting NAT would cause the loss of client network source IP addresses.
Out-of-path WAN optimization with inter-VDOM routing

Advanced configuration example

set nat enable
end
end

Configure other policy settings that you may require. For example, you could add a protection profile.

3 Add a firewall policy that allows all port5 to port4 FTP sessions:

```fortigateconf
config firewall policy
edit 2
set srcintf port5
set dstintf port4
set srcaddr all
set dstaddr all
set action accept
set service FTP
set schedule always
set nat enable
end
end
```

Configure other policy settings that you may require.

4 If required, use the `move` command to change the order of the policies in the policy list.

Follow the normal rules for ordering firewall policies in the policy list. For example, move specific rules above general rules. For more information about these rules, see the FortiGate Administration Guide.

5 Add a policy route to redirect HTTP traffic received at port5 to exit the FortiGate unit using port4. Set the gateway address of the route to 172.10.10.2 so that the HTTP sessions are directed to the FortiGate-311B port1 interface. For HTTP traffic, the protocol is 6 (TCP) and the destination port is 80:

```fortigateconf
config router policy
edit 1
set protocol 6
set input-device port5
set output-device port4
set src 0.0.0.0/0.0.0.0
set dst 0.0.0.0/0.0.0.0
set start-port 80
set end port 80
set gateway 172.10.10.2
```

Accept default settings for `tos (0x00)` and `tos-mask (0x00)`.

6 Add a policy route to redirect FTP traffic received at port5 to exit the FortiGate unit using port4. Set the gateway address of the route to 172.10.10.2 so that the FTP sessions are directed to the FortiGate-311B port1 interface. For FTP traffic, the protocol is 6 (TCP) and the destination port is 21:

```fortigateconf
config router policy
edit 1
set protocol 6
set input-device port5
set output-device port4
set src 0.0.0.0/0.0.0.0
set dst 0.0.0.0/0.0.0.0
```
Advanced configuration example

Out-of-path WAN optimization with inter-VDOM routing

set start-port 21
set end port 21
set gateway 172.10.10.2
end
end

Accept default settings for tos (0x00) and tos-mask (0x00).

To configure the FortiGate-311B unit for multiple VDOM operation and add an inter-VDOM link

1. Enable multiple VDOM operation and log back in to the web-based manager:
   config system global
   set vdom-admin enable
   end

2. Log back in to the CLI.

3. Add a new virtual domain named Wanopt.
   config vdom
   edit Wanopt
   end

4. Add the port10 interface to the Wanopt VDOM:
   config global
   config system interface
   edit port10
   set vdom Wanopt
   set IP 10.10.10.2/24
   end
   end

5. Add an inter-VDOM named Vlink and configure the Vlink0 and Vlink1 interfaces:
   config global
   config system vdom-link
   edit Vlink
   end
   config system interface
   edit Vlink0
   set vdom root
   set ip 172.1.1.1/24
   next
   edit Vlink1
   set vdom Wanopt
   set ip 172.1.1.2/24
   end
   end

To configure routing for the FortiGate-311B root VDOM

1. Log in to the root VDOM from the CLI.

2. Add a default route. The destination of the default route is the inter-VDOM link interface in the root VDOM. The gateway of the default route is the IP address of the inter-VDOM link interface in the Wanopt VDOM. The result is the default route sends all traffic out the inter-VDOM link and into the Wanopt VDOM:
   config router static
   edit 1
Out-of-path WAN optimization with inter-VDOM routing

Advanced configuration example

set dst 0.0.0.0/0.0.0.0
set device Vlink0
set gateway 172.1.1.2
set distance 10
end

3 Add a route to send return traffic from the server network destined for the client network out the port1 interface to the port4 interface of the FortiGate-300A which has IP address 172.10.10.1:

config router static
  edit 2
    set dst 172.20.120.0/24
    set device port1
    set gateway 172.10.10.1
    set distance 10
  end

To add firewall policies to the FortiGate-311B root VDOM to accept HTTP and FTP sessions received at port1 and destined for Vlink0 and apply a protection profile

1 Log in to the root VDOM from the CLI.

2 Add a firewall policy that accepts HTTP sessions received at port1 and applies a protection profile to them:

config firewall policy
  edit 20
    set srcintf port1
    set dstintf Vlink0
    set srcaddr all
    set dstaddr all
    set action accept
    set service HTTP
    set schedule always
    set profile-status enable
    set profile scan
  end

Tip: To preserve the source addresses of the HTTP sessions, NAT should not be enabled for this policy.

Tip: You can select any protection profile that you may require.

Configure other policy settings that you may require. You can also use more specific firewall addresses or add one firewall policy that accepts both FTP and HTTP traffic.

3 Add a firewall policy that accepts FTP sessions received at port1 and applies a protection profile to them:

config firewall policy
  edit 20
    set srcintf port1
    set dstintf Vlink0
    set srcaddr all
    set dstaddr all
    set action accept
set service FTP
set schedule always
set profile-status enable
set profile scan
end

Tip: To preserve the source addresses of the HTTP sessions, NAT should not be enabled for this policy.

Tip: You can select any required protection profile that you may require.

Configure other policy settings that you may require. You can also use more specific firewall addresses or add one firewall policy that accepts both FTP and HTTP traffic.

To configure routing for the FortiGate-311B Wanopt VDOM
1 Log in to the Wanopt VDOM from the CLI.
2 Add a default route. The destination of the default route is the port10 interface. The gateway of the default route is the next hop router that the port10 interface connects with:
   config router static
   edit 1
       set dst 0.0.0.0/0.0.0.0
       set device port10
       set gateway (next hop router IP address)
       set distance 10
   end
3 Add a route to send return traffic from the server network destined for the client network out the Vlink1 interface to the Vlink0 interface in the root VDOM, which has the IP address 172.1.1.2:
   config router static
   edit 2
       set dst 172.20.120.0/24
       set device Vlink1
       set gateway 172.1.1.2
       set distance 10
   end

To add firewall policies to the FortiGate-311B Wanopt VDOM to accept HTTP and FTP sessions received at the Vlink1 interface of the inter-VDOM link destined for port10
1 Log in to the Wanopt VDOM from the CLI.
2 Add a firewall policy that accepts HTTP sessions received at Vlink1 and destined for port10:
   config firewall policy
   edit 20
       set srcintf Vlink1
       set dstintf port10
       set srcaddr all
       set dstaddr all
set action accept
set service HTTP
set schedule always
set nat enable
end

Tip: NAT is ignored for all HTTP sessions for the server network because these sessions are intercepted by a full optimization WAN optimization rule. However, HTTP sessions for the Internet are intercepted by the Web Cache Only rule, so source NAT is required for replies.

Tip: Do not select a Protection Profile because you cannot apply a protection profile and WAN optimization to the same session in the same VDOM. A protection profile was applied to the session in the root VDOM.

Configure other settings that you may require.

3 Go to Firewall > Policy and select Create New to add a firewall policy that accepts FTP sessions received at Vlink1 and destined for port10:

```
config firewall policy
edit 20
  set srcintf Vlink1
  set dstintf port10
  set srcaddr all
  set dstaddr all
  set action accept
  set service FTP
  set schedule always
  set nat enable
end
```

Tip: NAT is ignored for all HTTP sessions for the server network because these sessions are intercepted by a full optimization WAN optimization rule. However, HTTP sessions for the Internet are intercepted by the Web Cache Only rule, so source NAT is required for replies.

Tip: Do not select a Protection Profile because you cannot apply a protection profile and WAN optimization to the same session in the same VDOM. A protection profile was applied to the session in the root VDOM.

Configure other settings that you may require.

**To configure peers for the FortiGate-311B Wanopt VDOM**

1 Log in to the Wanopt VDOM from the CLI.

2 Add the Local Host ID for the client-side FortiGate-311B unit:

```
config wanopt settings
  set host-id Client_Fgt
end
```

3 Add a Peer Host ID and the IP Address for the server-side FortiGate-620B unit.

```
config wanopt peer
  edit Server_Fgt
  set ip 10.20.20.2
end
```
To add WAN optimization rules for HTTP and FTP to the FortiGate-311B Wanopt VDOM

1. Log in to the Wanopt VDOM from the CLI.
2. Add an active rule to optimize HTTP traffic from IP addresses on the Client network (172.20.120.0) with a destination address on the server network (192.168.10.0):

   ```
   config wanopt rule
   edit 4
   set auto-detect active
   set src-ip 172.20.120.0-172.20.120.255
   set dst-ip 192.168.10.0-192.168.10.255
   set port 80
   set proto http
   end
   
   Accept default settings for transparent (enable), status (enable), mode (full), byte-caching (enable), ssl (disable), secure-tunnel (disable), auth-group (null), unknown-http-version (tunnel), and tunnel-non-http (disable).
   ```

   **Tip:** For improved privacy you can enable secure-tunnel and add an authentication group to both optimizing FortiGate units.

3. Add an active rule to optimize FTP traffic from IP addresses on the Client network (172.20.120.0) with a destination address on the server network (192.168.10.0):

   ```
   config wanopt rule
   edit 5
   set auto-detect active
   set src-ip 172.20.120.0-172.20.120.255
   set dst-ip 192.168.10.0-192.168.10.255
   set port 21
   set proto ftp
   end
   
   Accept default settings for transparent (enable), status (enable), mode (full), byte-caching (enable), ssl (disable), secure-tunnel (disable), auth-group (null), unknown-http-version (tunnel), and tunnel-non-http (disable).
   ```

   **Tip:** For improved privacy you can enable secure-tunnel and add an authentication group to both optimizing FortiGate units.

4. Add a rule to web cache HTTP traffic from IP addresses on the Client network (172.20.120.0) with any destination address:

   ```
   config wanopt rule
   edit 6
   set mode webcache-only
   set src-ip 172.20.120.0-172.20.120.255
   set dst-ip 0.0.0.0
   set port 80
   set proto http
   ```
Accept default settings for transparent (enable), status (enable), ssl (disable), unknown-http-version (tunnel), and tunnel-non-http (disable).

5 If required, use the move command to move the Web Cache Only rule below the full optimization HTTP and FTP rules in the list. The Web Cache Only rule should be below the full optimization rules because it will match all HTTP traffic and you need HTTP sessions with destination address 192.168.10.0 to match the full optimization HTTP rule.

For more information, see “Moving a rule to a different position in the rule list” on page 41.

Server-side configuration steps - CLI

This section describes the configuration steps required for the server-side FortiGate-620B unit to perform WAN optimization with the client-side FortiGate-311B unit and to send HTTP and FTP sessions to the server-side FortiGate-1000A cluster. This section also describes how to configure the FortiGate-1000A cluster to forward HTTP and FTP sessions from the client network to the server network.

The section breaks down the client-side configuration into smaller procedures. For best results, follow the procedures in the order given:

1 Configure routing for the FortiGate-620B unit.
2 Configure peers for the server-side FortiGate-620B unit.
3 Add a passive WAN optimization rule to the server-side FortiGate-620B unit.
4 Configure the FortiGate-1000A cluster to accept HTTP and FTP connections at port5 and forward them out port1 to the server network.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

To configure routing for the FortiGate-620B unit

1 Add a default route. The destination of the default route is the port16 interface. The gateway of the default route is the next hop router that the port16 interface connects with:

```
config router static
edit 1
  set dst 0.0.0.0/0.0.0.0
  set device port16
  set gateway (next hop router IP address)
  set distance 10
end
```

2 Add a route to send traffic for the server network out port1 to the port5 interface of the FortiGate-1000A cluster, which has the IP address 192.20.20.1:

```
config router static
edit 2
  set dst 192.168.10.0/24
  set device port1
  set gateway 192.20.20.1
  set distance 10
end
```
To configure peers for the server-side FortiGate-620B unit

1. Add the Local Host ID for the server-side FortiGate-620B unit:
   ```
   config wanopt settings
   set host-id Server_Fgt
   end
   ```

2. Add a Peer Host ID and the IP Address for the client-side FortiGate-311B unit:
   ```
   config wanopt peer
   edit Client_Fgt
   set ip 10.10.10.2
   end
   ```

To add a passive WAN optimization rule to the server-side FortiGate-620B unit

You can add one passive WAN optimization rule to the server-side FortiGate-620B unit for both active rules on the FortiGate-311B unit. This rule can also allow the FortiGate-620B to perform WAN optimization with other client-side devices as long as the required Peer Host IDs are added to the FortiGate-620B configuration and to the client-side configurations.

1. Go to WAN Opt. & Cache > Rule and select Create New to add a passive rule that accepts any WAN optimization tunnel request:
   ```
   config wanopt rule
   edit 5
   set auto-detect passive
   set src-ip 0.0.0.0
   set dst-ip 192.168.10.0-192.168.10.255
   set port 1-65535
   set webcache enable
   end
   ```
   Accept default settings for status (enable) and mode (full).

Tip: You can also use a narrower port range such as 21-80 or add two rules, one with port set to 80 and one with port set to 21.

2. If required, use the move command to move the rule to a different position in the list so that the tunnel request from the client-side FortiGate unit matches with this rule.
   For more information, see “Moving a rule to a different position in the rule list” on page 41.

To configure the FortiGate-1000A cluster to accept HTTP and FTP connections at port5 and forward them out port1 to the server network

1. Add a firewall address for the server network:
   ```
   config firewall address
   edit Server_Net
   set type iprange
   set start-ip 192.168.10.0
   set end-ip 192.168.10.255
   end
   ```

2. Add a firewall address for the client network:
   ```
   config firewall address
   edit Client_Net
   set type iprange
   ```

Tip: You can also use a narrower port range such as 21-80 or add two rules, one with port set to 80 and one with port set to 21.
set start-ip 172.20.120.0
set end-ip 172.20.120.255
end

3 Go to Firewall > Policy and select Create New to add a firewall policy that accepts HTTP sessions at port5 destined for port1 and the server network:

```
cfg firewall policy
ed 10
    set srcintf port5
    set dstintf port1
    set srcaddr Client_Net
    set dstaddr Server_Net
    set action accept
    set service HTTP
    set schedule always
end
```
end

Tip: WAN optimization is operating in Transparent mode so the packets from the client network include their client network source IP addresses. To preserve these source IP addresses, the firewall policies on the FortiGate-1000A cluster that accept the sessions from the FortiGate-620B unit should not apply NAT. If the policies were to apply NAT, the client network addresses would be replaced with the port1 IP address of the FortiGate-1000A cluster and the client network source IP addresses would be lost.

4 Go to Firewall > Policy and select Create New to add a firewall policy that accepts FTP sessions at port5 destined for port1 and the server network:

```
cfg firewall policy
ed 11
    set srcintf port5
    set dstintf port1
    set srcaddr Client_Net
    set dstaddr Server_Net
    set action accept
    set service FTP
    set schedule always
end
```
end

Tip: As described above, selecting NAT would cause the loss of the client network source IP addresses.
SSL offloading for WAN optimization and web caching

WAN optimization SSL offloading uses the FortiGate unit to encrypt and decrypt SSL sessions. WAN optimization supports SSL offloading for HTTP and HTTPS sessions to and from web servers. The FortiGate unit intercepts HTTPS traffic from clients and decrypts it before sending it as HTTP clear text to the web server. The HTTP clear text response from the web server is encrypted by the FortiGate unit and returned to the client as an HTTPS session. The result should be a performance improvement because SSL encryption and decryption is offloaded from the server to the FortiGate unit’s FortiASIC SSL encryption/decryption engine. You can also combine SSL offloading with other WAN optimization techniques such as HTTP protocol optimization, byte caching, and web caching to further enhance web server performance.

You enable SSL offloading by selecting Enable SSL in a WAN optimization rule. You must also add SSL servers to support SSL offloading by using the CLI command `config wanopt ssl-server`.

You must add one WAN optimization SSL server configuration to a FortiGate unit for each HTTP server for which you are configuring SSL offloading. This SSL server configuration must also include the HTTP server CA. You load this certificate into the FortiGate unit as a local certificate and then add it to the SSL server configuration using the `ssl-cert` keyword. The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.

You can configure one WAN optimization rule to offload SSL encryption/decryption for multiple HTTP servers. To do this, you configure the WAN optimization rule source and destination addresses, so that the rule accepts packets destined for all of the HTTP servers for which you want offloading. Then you add one SSL server configuration for each of the HTTP servers.

A number of SSL offloading configurations are possible. This chapter demonstrates two:

- Example: SSL offloading for a WAN optimization tunnel
- Example: SSL offloading and reverse proxy web caching for an Internet web server

**Example: SSL offloading for a WAN optimization tunnel**

This example shows how to configure basic SSL offloading for a WAN optimization tunnel. This basic SSL offloading configuration can be applied to many network configurations.

**Network topology and assumptions**

In this example, clients on a client network use `https://192.168.10.20` to browse to a web server. A WAN optimization rule with `Auto-Detect` set to `Off` on the client-side FortiGate unit accepts sessions from the clients with source addresses on the 172.20.120.0 network and with a destination address of 192.168.10.0 and a destination port of 443. In this rule, `Enable Secure Tunnel` is selected so that the tunnel is encrypted. To support the encrypted tunnel, the configuration also includes an authentication group with a pre-shared key. Both FortiGate units must have the same authentication group with the same pre-shared key.
The server-side FortiGate unit includes an SSL server configuration with `ip` set to 192.168.10.20 and `port` to 443. The unit also includes the web server CA.

**Figure 41: SSL offloading WAN optimization configuration**

When the client-side FortiGate unit accepts an HTTPS connection for 192.168.10.20, the SSL server configuration provides the information that the client-side unit needs to decrypt the traffic and send it in clear text across a WAN optimization tunnel to the server-side unit. The server-side unit then forwards the clear text packets to the web server.

The web server CA is not downloaded from the server side to the client-side FortiGate unit. Instead, the client-side FortiGate unit proxies the SSL parameters from the client side to the server side, which returns an SSL key and other required information to the client-side unit so that it can decrypt and encrypt HTTPS traffic.

**Note:** In this peer-to-peer configuration you do not need to add a WAN optimization rule to the server-side FortiGate unit as long as this server-side unit includes the peer host ID of the client-side FortiGate unit in its peer list. However, you can set Auto-Detect to Active on the client-side FortiGate unit and then add a passive rule to the server-side unit.

In this example, you do not require the secure tunnel and the authentication group configurations, but they are included to show how to protect the privacy of the WAN optimization tunnel. Alternatively, you could configure a route-based IPSec VPN between the FortiGate units and use IPSec to protect the privacy of the WAN optimization tunnel.

In this example, it is assumed that you have a local CA named `Web_Server_Cert_1.crt` stored in a file that you will import when you configure the server-side FortiGate unit.

**General configuration steps**

This example is divided into client-side and server-side steps, as configured through the web-based manager, and with CLI instructions provided for CLI-only steps. For best results, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

You also need access to the CLI to perform CLI-only steps.

**Client-side configuration steps**

1. Go to **WAN Opt. & Cache > Peer** and enter a **Local Host ID** for the server-side FortiGate unit:
SSL offloading for WAN optimization and web caching

Example: SSL offloading for a WAN optimization tunnel

Local Host ID User_net

2 Select Apply to save your setting.

3 Select Create New and add a Peer Host ID and the IP Address for the peer side FortiGate unit:

   Peer Host ID Web_servers
   IP Address 192.168.10.1

4 Select OK.

5 Go to WAN Opt. & Cache > Peer > Authentication Group and select Create New to add an authentication group named SSL_auth_grp to the client-side FortiGate unit.

   The authentication group includes a pre-shared key and the peer added in step 3. An authentication group with the same name and the same pre-shared key must also be added to the server-side FortiGate unit. This authentication group is required for the secure tunnel:

   Name SSL_auth_grp
   Authentication Method Pre-shared key
   Password <pre-shared_key>
   Peer Acceptance Specify Peer: Web_servers

6 Select OK.

7 Go to WAN Opt. & Cache > Rule and select Create New to add the WAN optimization rule:

   Mode Full Optimization
   Source 172.20.120.*
   Destination 192.168.10.*
   Port 443
   Auto-Detect Off
   Protocol HTTP
   Peer Web_servers
   Transparent Mode Select
   Enable Byte Caching Select
   Enable SSL Select
   Enable Secure Tunnel Select
   Authentication Group SSL_auth_grp

8 Select OK.

   The rule is added to the bottom of the WAN optimization list.

9 If required, move the rule to a different position in the list.

   The order of the rules in the list significantly affects how the rules are applied. For more information, see "How list order affects rule matching" on page 40 and "Moving a rule to a different position in the rule list" on page 41.
Server-side configuration steps

To configure the server-side FortiGate unit

1. Go to WAN Opt. & Cache > Peer and enter a Local Host ID for the server-side FortiGate unit:
   - Local Host ID: Web_servers

2. Select Apply to save your setting.

3. Select Create New and add a Peer Host ID and the IP Address for the peer side FortiGate unit:
   - Peer Host ID: User_net
   - IP Address: 172.20.120.1

4. Select OK.

5. Go to WAN Opt. & Cache > Peer > Authentication Group and select Create New to add an authentication group named SSL_auth_grp to the server-side FortiGate unit. The authentication group includes a pre-shared key and the peer added to the server-side FortiGate unit in step 3:
   - Name: SSL_auth_grp
   - Authentication Method: Pre-shared key
   - Password: <pre-shared_key>
   - Peer Acceptance: Specify Peer: User_net

6. Select OK.

7. Go to System > Certificates > Local Certificates and select Import to import the web server’s CA.
   - For Type, select Local Certificate. Select the Browse button to locate the file, Web_Server_Cert_1.crt.
   - The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.

8. From the CLI, enter the following command to add the SSL server to the server-side FortiGate unit:
   ```plaintext
cfg wanopt ssl-server
edit example_server
set ip 192.168.10.20
set port 443
set ssl-cert Web_Server_Cert_1
end
```
   - Configure other ssl-server settings that you may require for your configuration.

Example: SSL offloading and reverse proxy web caching for an Internet web server

This example shows how to configure SSL offloading for a reverse proxy Web Cache Only WAN optimization configuration.
Network topology and assumptions

In this configuration, clients on the Internet use HTTPS to browse to a web server. The FortiGate unit intercepts the HTTPS traffic, and a Web Cache Only WAN optimization rule with SSL offloading enabled decrypts the traffic before sending it to the web server. The FortiGate unit also caches pages from the web server. Replies from the web server are encrypted by the FortiGate unit before returning to the web browsing clients.

The Web Cache Only rule enables transparent mode because the FortiGate unit is performing NAT between the Internet and the HTTP server and the web server network is not configured to route Internet traffic between the FortiGate unit and the web server.

In this configuration, the FortiGate unit is operating in reverse proxy mode. Reverse proxy caches can be placed directly in front of a particular server. Web caching on the FortiGate unit reduces the number of requests that the web server must handle, therefore leaving it free to process new requests that it has not serviced before.

Using a reverse proxy configuration:

- avoids the capital expense of additional web servers by increasing the capacity of existing servers
- serves more requests for static content from web servers
- serves more requests for dynamic content from web servers
- reduces operating expenses including the cost of bandwidth required to serve content
- accelerates the response time of web servers and of page download times to end users.

When planning a reverse proxy implementation, the web server's content should be written so that it is “cache aware” to take full advantage of the reverse proxy cache.

In reverse proxy mode, the FortiGate unit functions more like a web server for the clients it services. Unlike internal clients, external clients are not reconfigured to access the proxy server. Instead, the site URL routes the client to the FortiGate unit as if it were a web server. Replicated content is delivered from the proxy cache to the external client without exposing the web server or the private network residing safely behind the firewall.

In this example, the site URL translates to IP address 192.168.10.1, which is the port2 IP address of the FortiGate unit. The port2 interface is connected to the Internet.

This example also includes two Web Cache Only rules, one that accepts the HTTP traffic for web caching and one that accepts the HTTPS traffic for SSL offloading and web caching. You could instead add only one rule for both the HTTP and HTTPS traffic.

For this example, it is also assumed that all HTTP traffic uses port 80 and all HTTPS traffic uses port 443.

The FortiGate unit includes the web server CA and an SSL server configuration for IP address 172.10.20.30 and port to 443. The name of the file containing the CA is Rev_Proxy_Cert_1.crt.
Configuration steps

To configure the FortiGate unit as a reverse proxy web cache server

1. Go to Firewall > Virtual IP and select Create New to add a virtual IP that translates the destination IP address from 192.168.10.1 to 172.10.20.30:

   - Name: Reverse_proxy_VIP
   - External Interface: port2
   - Type: Read only description of currently mode, usually Static NAT.
   - External IP Address/Range: 192.168.10.1
   - Mapped IP Address/Range: 172.10.20.30
   - Port Forwarding: Do not select.

2. Select OK to save your settings.

3. Go to Firewall > Policy and select Create New to add a port2 to port1 firewall policy that accepts HTTP and HTTPS traffic from the Internet:

   - Do not select a protection profile. Set the destination address to the virtual IP. You do not have to enable NAT.

   - Source Interface/Zone: port2
   - Source Address: all
   - Destination Interface/Zone: port1
   - Destination Address: Reverse_proxy_VIP
   - Service: HTTP and HTTPS
     
   - Note: Select Multiple to display a screen for entering more than one service.

   - Action: ACCEPT

4. Select OK to save your settings.

5. Go to WAN Opt. & Cache > Rule and select Create New to add a Web Cache Only WAN optimization rule.

6. Configure the rule to accept the HTTP traffic accepted by the firewall policy:
SSL offloading for WAN optimization and web caching  Example: SSL offloading and reverse proxy web caching for an Internet web

To configure the FortiGate unit for SSL offloading of HTTPS traffic

2. Configure the rule to accept the HTTPS traffic accepted by the firewall policy:

   - Mode: Web Cache Only
   - Source: 0.0.0.0
   - Destination: 192.168.10.1
   - Port: 80
   - Transparent Mode: Select
   - Enable SSL: Do not select

   7. Select OK.
   - The rule is added to the bottom of the WAN optimization list.

   8. If required, move the rule to a different position in the list.
   - The order of the rules in the list significantly affects how the rules are applied. For more information, see “How list order affects rule matching” on page 40 and “Moving a rule to a different position in the rule list” on page 41.

To add an SSL server to offload SSL encryption and decryption for the web server.

1. Go to System > Certificates > Local Certificates and select Import to import the web server’s CA.
   - For Type, select Local Certificate. Select the Browse button to locate the file Rev_Proxy_Cert_1.crt.
   - The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.
2. From the CLI, enter the following command to add the SSL server.

   Mode: Web Cache Only
   Source: 0.0.0.0
   Destination: 192.168.10.1
   Note: You need to set Destination to the IP address that is translated by the virtual IP (192.168.10.1) and not to the server IP (172.10.20.30).
   Port: 443
   Transparent Mode: Select.
   Enable SSL: Select.

   7. Select OK.
   - The rule is added to the bottom of the WAN optimization list.

   8. If required, move the rule to a different position in the list.
   - The HTTPS rule can be above or below the HTTP rule.
   - The order of the rules in the list significantly affects how the rules are applied. For more information, see “How list order affects rule matching” on page 40 and “Moving a rule to a different position in the rule list” on page 41.
3 Configure other `ssl-server` settings that you may require for your configuration.

The order of the rules in the list significantly affects how the rules are applied. For more information, see “How list order affects rule matching” on page 40 and “Moving a rule to a different position in the rule list” on page 41.

```plaintext
config wanopt ssl-server
  edit rev_proxy_server
    set ip 172.10.20.30
    set port 443
    set ssl-cert Rev_Proxy_Cert_1
  end
```
FortiClient WAN optimization

FortiClient WAN optimization works together with WAN optimization on a FortiGate unit to accelerate network traffic between a PC running version 4.0 or greater of the FortiClient application and a network behind a FortiGate unit. When a user of a PC with FortiClient WAN optimization enabled attempts to connect to network resources behind a server-side FortiGate unit, the FortiClient application automatically detects if WAN optimization is enabled on the FortiGate unit. If WAN optimization is detected and the FortiClient application can successfully negotiate a WAN optimization tunnel with the FortiGate unit, a WAN optimization tunnel starts.

FortiClient WAN optimization includes protocol optimization settings selected in the FortiClient application and byte caching (byte caching is enabled by default in the FortiClient application and cannot be disabled). Web caching is applied if selected in the passive rule on the FortiGate unit that accepts FortiClient WAN optimization tunnel requests.

This chapter describes how to configure the FortiClient application for WAN optimization and how to configure a FortiGate unit to accept WAN optimization tunnel requests from the FortiClient application.

Figure 43: FortiClient WAN optimization topology

Configuring FortiClient WAN optimization

Configuring WAN optimization with the FortiClient application consists of enabling WAN optimization for the FortiClient application and configuring the FortiGate unit to accept WAN optimization tunnel requests from the FortiClient application.

FortiClient configuration steps

To configure WAN Optimization for the FortiClient application

1. From the FortiClient user interface, go to Status > WAN Optimization.
2. Select Enable WAN Optimization.
3 Enable the protocols to be optimized: HTTP (web browsing), CIFS (Windows file sharing), MAPI (Microsoft Exchange) and FTP (file transfers).

4 Set Maximum Disk Cache to 512, 1024, or 2048 MB.
   The default is 512 MB. If the PC hard disk can accommodate a larger cache, better optimization performance is possible.

5 Select Apply.

FortiGate unit configuration steps

To configure FortiClient WAN Optimization on the FortiGate unit

Because PCs running the FortiClient application can have IP addresses that change often, it is usually not practical to add PCs running the FortiClient application to the WAN optimization peer list. Instead, a FortiGate unit that accepts WAN optimization tunnel requests from the FortiClient application should be configured to accept any peer (see “Accepting any peers” on page 29) by adding an authentication group named auth-fc with Peer acceptance set to Accept Any Peer.

On the FortiGate unit, you also need to add a passive rule that includes source and destination addresses that will accept connections from the IP addresses of PCs running the FortiClient application. If these PCs can be anywhere on the Internet, the source address for this rule is 0.0.0.0. You can also use a more restrictive address range if the PCs running the FortiClient application have a restricted range of addresses.

You do not need to add firewall policies to the FortiGate unit because it is on the server side of the WAN optimization tunnel.

1 Go to WAN Opt. & Cache > Peer > Authentication Group and select Create New.

2 Configure the authentication group:

   Name: auth-fc
   Authentication Method: Certificate
   Certificate: Fortinet_Firmware
   Peer Acceptance: Accept Any Peer

3 Select OK.

4 Go to WAN Opt. & Cache > Rule and select Create New.

5 Configure a rule to accept FortiClient WAN optimization sessions:

   Mode: Full Optimization
   Source: 0.0.0.0
   Destination: 0.0.0.0
   Port: 1-65535
   Auto-Detect: Passive

6 Select OK.
The FortiGate explicit web proxy

You can use the FortiGate web proxy and interface settings to enable explicit HTTP and HTTPS proxying on one or more FortiGate interfaces. When enabled, the FortiGate unit becomes an explicit web proxy server. All HTTP and HTTPS session received by interfaces with explicit web proxy enabled are intercepted by the explicit web proxy and relayed to their destinations.

Routing determines the FortiGate interface that the proxied packets exit the FortiGate unit from. For example, you could enable the explicit proxy on the internal interface to proxy internal users connections to the Internet. HTTP and HTTPS sessions destined for the Internet would be received by the explicit web proxy at the internal interface. These sessions would then be routed using the default route and exit the FortiGate unit external interface before proceeding to the destination on the Internet.

The source address of packets exiting the FortiGate unit becomes the IP address of the FortiGate interface that the packets exit from. In the example described in the previous paragraph, the source address of the exiting packets would be the source address of the external interface of the FortiGate unit.

To use the explicit proxy, users must add the IP address of a FortiGate interface on which the explicit proxy is enabled and the explicit proxy port number to the proxy configuration settings of their web browsers.

On FortiGate units that support WAN optimization, you can also enable web caching for the explicit proxy. For more information, see “Web caching” on page 63.

Applying protection profiles to explicit web proxy traffic

To enable protection profiles for explicit web proxy traffic, you must configure two VDOMs and use inter-VDOM routing to pass the web traffic between them. WAN optimization has a similar requirement, see “Out-of-path WAN optimization with inter-VDOM routing” on page 81 for an example WAN optimization configuration that uses inter-VDOM links. In the web proxy configuration you must enable the explicit web proxy on the inter-VDOM links. Then traffic is accepted by a VDOM that applies virus scanning. Then the web traffic is picked up by the web proxy at the inter-VDOM link. You cannot enable the explicit web proxy for an inter-VDOM link from the web-based manager. Instead you must use the following CLI command. For example, for an inter-VDOM link interface named Vlink0:

```
config system interface
  edit Vlink0
    set explicit-web-proxy enable
end
```

Configuring the explicit web proxy

To enable explicit proxy on an interface, go to System > Network > Interface, select the interface, and enable explicit web proxy.

Caution: Enabling the explicit web proxy on an interface connected to the Internet is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address.
To configure the explicit web proxy go to System > Network > Web Proxy.

**Figure 44: Configuring Web Proxy settings**

<table>
<thead>
<tr>
<th>Web Proxy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy FQDN</td>
<td>default.fqdn</td>
</tr>
<tr>
<td>Max HTTP request length</td>
<td>4 Kb</td>
</tr>
<tr>
<td>Max HTTP message length</td>
<td>50 Kb</td>
</tr>
<tr>
<td>Add Headers to Forwarded Requests</td>
<td></td>
</tr>
<tr>
<td>Client IP Header</td>
<td>Enable</td>
</tr>
<tr>
<td>Via Header</td>
<td>Enable</td>
</tr>
<tr>
<td>X-forwarded-for Header</td>
<td>Enable</td>
</tr>
<tr>
<td>Front-end HTTPS Header</td>
<td>Enable</td>
</tr>
<tr>
<td>Explicit Web Proxy Options</td>
<td>Enable Explicit Web Proxy</td>
</tr>
<tr>
<td>Port</td>
<td>8080</td>
</tr>
<tr>
<td>Listen on Interfaces</td>
<td>None</td>
</tr>
<tr>
<td>Unknown HTTP version</td>
<td>Reject</td>
</tr>
<tr>
<td><strong>Apply</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Proxy FQDN**
Enter the fully qualified domain name (FQDN) for the proxy server. This is the domain name to enter into browsers to access the proxy server.

**Max HTTP request length**
Enter the maximum length of an HTTP request. Larger requests will be rejected.

**Max HTTP message length**
Enter the maximum length of an HTTP message. Larger messages will be rejected.

**Add headers to Forwarded Requests**
The web proxy server will forward HTTP requests to the internal network. You can include the following headers in those requests:

- **Client IP Header**
  - Enable to include the Client IP Header from the original HTTP request.

- **Via Header**
  - Enable to include the Via Header from the original HTTP request.

- **X-forwarded-for Header**
  - Enable to include the X-Forwarded-For (XFF) HTTP header.
  - The XFF HTTP header identifies the originating IP address of a web client or browser that is connecting through an HTTP proxy, and the remote addresses it passed through to this point.

- **Front-end HTTPS Header**
  - Enable to include the Front-end HTTP Header from the original HTTPS request.

**Explicit Web Proxy Options**

- **Enable Explicit Web Proxy**
  - Enable the explicit web proxy server. You must select this option for the explicit web proxy to accept and forward packets.

- **Port**
  - Enter the explicit web proxy server port, for example 8080. To use the explicit proxy, users must add this port to their web browser proxy configuration.

- **Listen on Interfaces**
  - Displays the interfaces that are being monitored by the explicit web proxy. If VDOMs are enabled, only interfaces that belong to the current VDOM and have explicit web proxy enabled will be displayed. If you enable the web proxy on an interface that has VLANs on it, the VLANs will only be enabled for web proxy if you manually enable each of them.

- **Unknown HTTP version**
  - Select the action to take when the proxy server must handle an unknown HTTP version request or message. Choose from either Reject or Best Effort. The Reject option is more secure.
Example: Explicit proxy configuration

This example describes how to configure the explicit proxy for users on a network connected to the port1 FortiGate unit interface. The example also involves setting the explicit proxy port to 8888 and enabling web caching for the web proxy.

You need to enable explicit web proxy on one or more FortiGate interfaces. Explicit proxy users must configure their web browsers to connect to a proxy server. In this example, the proxy server IP address that users would add to their web browsers is the IP address of the port1 FortiGate interface and the proxy server port would be 8888. If the FortiGate unit is operating in Transparent mode the proxy server IP address would be the management address of the FortiGate unit.

In this configuration, VDOMs are not enabled.

General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Enable the explicit proxy on one or more interfaces.
2. Enable and configure the explicit proxy.
3. Enable web caching for the explicit proxy.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

Configuring the explicit web proxy - web-based manager

Use the following steps to configure the example web proxy configuration from FortiGate unit web-based manager. (CLI steps follow.)

To enable the explicit web proxy on the port1 interface - web-based manager

1. Go to System > Network > Interface.
2. Select the port interface.
4. Select Apply.

You can also optionally enable the explicit web proxy on other interfaces.

When you go to System > Network > Web Proxy, under Explicit Web Proxy Options, beside Listen on Interfaces, you will see the port1 interface and any other interfaces that you enabled.

Note: Only interfaces that have explicit web proxy enabled and are in the current VDOM will be displayed. If an interface has a VLAN subinterface configured, it must be enabled separately for explicit web proxy. Enabled interfaces will be displayed independent of explicit web proxy being enabled or not on the Web Proxy screen.

To enable and configure the explicit web proxy - web-based manager

2. Select Enable Explicit Proxy.
3. Set Port to 8888.
4. Select Apply.
To enable web caching for the explicit web proxy

You can enable web caching for the explicit web proxy on FortiGate units that support WAN optimization and web caching. For more information, see “Web caching” on page 63.

2. Select Apply.

Web content requested by users using the explicit proxy are now cached by the FortiGate unit using the WAN optimization web cache.

Configuring the explicit web proxy - CLI

Use the following steps to configure the example web proxy configuration from FortiGate unit CLI steps follow.

To enable the explicit web proxy and web caching on the port1 interface - CLI

1. Enable the explicit web proxy on the FortiGate port1 interface so that users can use this interface and its IP address as an explicit proxy server for their web browsers.

   config system interface
   edit port1
   set explicit-web-proxy enable
   end

2. Enable the explicit proxy and set the TCP port that proxy accepts connections on to 8080.

   config web-proxy explicit
   set status enable
   set http-incoming-port 8888
   end

   The result of this configuration is that TCP sessions received by the FortiGate unit at port1 with a destination port number of 8888 are processed by the explicit web proxy.

3. Enable web caching for the explicit web proxy on FortiGate units that support WAN optimization and web caching.

   config wanopt webcache
   set explicit enable
   end

CLI configuration

config web-proxy explicit

Use the config web-proxy explicit command to configure an explicit web proxy.

Syntax

config web-proxy explicit
   set http-incoming-port <port_num>
   set status {enable | disable}
   set unknown-http-version {best-effort | reject}
end
config web-proxy global

Use the `config web-proxy global` command to configure global web proxy settings.

**Syntax**

```
config web-proxy global
  set add-header-client-ip {enable | disable}
  set add-header-front-end-https {enable | disable}
  set add-header-via {enable | disable}
  set add-header-x-forwarded-for {enable | disable}
  set max-message-length <kBytes>
  set max-request-length <kBytes>
  set proxy-fqdn <fqdn>
end
```

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>http-incoming-port &lt;port_num&gt;</td>
<td>Select the port the incoming HTTP traffic will use. Valid numbers range from 0 to 65535.</td>
<td></td>
</tr>
<tr>
<td>status {enable</td>
<td>disable}</td>
<td>Enable to activate explicit web proxies. When disabled, passive web proxies are used.</td>
</tr>
<tr>
<td>unknown-http-version {best-effort</td>
<td>reject} Select the action to take when an unknown version of HTTP is encountered.</td>
<td>reject</td>
</tr>
<tr>
<td>http-incoming-port &lt;port_num&gt;</td>
<td>Select the port the incoming HTTP traffic will use. Valid numbers range from 0 to 65535.</td>
<td></td>
</tr>
<tr>
<td>status {enable</td>
<td>disable}</td>
<td>Enable to activate explicit web proxies. When disabled, passive web proxies are used.</td>
</tr>
<tr>
<td>unknown-http-version {best-effort</td>
<td>reject} Select the action to take when an unknown version of HTTP is encountered.</td>
<td>reject</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>add-header-client-ip {enable</td>
<td>disable} Enable to add the client IP to the header of forwarded requests</td>
<td>disable</td>
</tr>
<tr>
<td>add-header-front-end-https {enable</td>
<td>disable} Enable to add a front-end-https header to forwarded requests.</td>
<td>disable</td>
</tr>
<tr>
<td>add-header-via {enable</td>
<td>disable} Enable to add the via header to forwarded requests.</td>
<td>disable</td>
</tr>
<tr>
<td>add-header-x-forwarded-for {enable</td>
<td>disable} Enable to add x-forwarded-for header to forwarded requests.</td>
<td>disable</td>
</tr>
<tr>
<td>max-message-length &lt;kBytes&gt;</td>
<td>Set the maximum length, in KB, of the HTTP message not including body. Range 16 to 256.</td>
<td>32</td>
</tr>
<tr>
<td>max-request-length &lt;kBytes&gt;</td>
<td>Set the maximum length, in kBytes, of the HTTP request line. Range 2 to 64.</td>
<td>4</td>
</tr>
<tr>
<td>proxy-fqdn &lt;fqdn&gt;</td>
<td>Set the fully qualified domain name (FQDN) for the proxy. This is the domain that clients connect to.</td>
<td>default.fqdn</td>
</tr>
</tbody>
</table>
WAN optimization storage

WAN optimization storage is used for storing the web cache and byte cache databases. In most cases, you can accept the default storage configuration.

You only have to configure WAN optimization storage if you have more than one possible storage location. This can happen if you have multiple storage locations or if you create multiple partitions on one storage device. When you add a second storage location, you must configure the FortiGate unit to use it for web caching, byte caching or both. You configure WAN optimization storage from the FortiGate CLI.

You can also override the default storage configuration if you only have one storage location but want to customize how WAN optimization uses the storage device. For example, if you have a relatively large storage device you may want to customize how the partitions on the device are used.

This chapter contains the following topics:

- Configuring WAN optimization storage
- Example: WAN optimization storage on a FortiGate-111C unit with two hard disks
- About partition labels

Configuring WAN optimization storage

You use the `execute scsci dev` CLI command as part of a WAN optimization configuration to edit FortiGate SCSI devices that can include internal high-capacity hard drives, AMC module hard drives, FSM devices. Unless you have to use more than one SCSI device or partition for WAN optimization, you do not need to change the SCSI device configuration.

To configure SCSI devices for WAN optimization:

1. Use the `execute scsi-dev partition` command to create and edit partitions.
2. Use the `execute scsi-dev storage` command to create WAN optimization storages. WAN optimization storages are logical parts of a partition used by WAN optimization to store the byte cache and web cache databases. You can create multiple storages but only two of them are used at a time—one for byte caching and one for web caching. You cannot use the same storage for both byte caching and web caching. You can add more than one storage to a partition.
3. Use the `config wanopt cache-storage` command to configure the storages for byte caching and web caching.

You can use the `show wanopt storage` command to view the storages that you have added. You can also use the `config wanopt storage` command to change the storage sizes.

**Syntax**

```
execute scsi-dev list
execute scsi-dev partition create <device_ref_int> <partition_size_int>
execute scsi-dev partition delete <partition_ref_int>
```
execute scsi-dev partition resize <partition_ref_int> <partition_size_int>
execute scsi-dev storage <partition_ref_int> <storage_size_int> <storage_name_str>

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>List the SCSI devices and partitions. The list displays device reference numbers &lt;device_ref_int&gt;, partition reference numbers &lt;partition_ref_int&gt;, and partition sizes &lt;partition_size_int&gt;.</td>
</tr>
<tr>
<td>partition create</td>
<td>Create new SCSI device partitions.</td>
</tr>
<tr>
<td>partition delete</td>
<td>Delete SCSI device partitions.</td>
</tr>
<tr>
<td>partition resize</td>
<td>Expand or shrink a SCSI device partition. Only the last partition on a device can be resized.</td>
</tr>
<tr>
<td>&lt;device_ref_int&gt;</td>
<td>SCSI device reference number displayed by the execute scsi-dev list command. These numbers uniquely identify each SCSI device.</td>
</tr>
<tr>
<td>&lt;partition_ref_int&gt;</td>
<td>Partition reference number displayed by the execute scsi-dev list command. These numbers uniquely identify each SCSI device partition.</td>
</tr>
<tr>
<td>&lt;partition_size_int&gt;</td>
<td>The size of a partition in MB.</td>
</tr>
<tr>
<td>&lt;storage_size_int&gt;</td>
<td>The size of a WAN optimization storage in MB. The storage can be from 16 MB up to the size of the partition.</td>
</tr>
<tr>
<td>&lt;storage_name_str&gt;</td>
<td>The name of the WAN optimization storage.</td>
</tr>
</tbody>
</table>

Examples

Use the following command to list the SCSI devices for a FortiGate unit that includes a FortiGate-ASM-S08 module.

#execute scsi-dev list

Device 1 492.0 MB ref:
  0 (Vendor: Model: USB DISK 2.0 Rev: PMAP)
    partition 1 39.1 MB ref: 1 label: <none>
    partition 2 39.1 MB ref: 2 label: <none>
    partition 3 39.1 MB ref: 3 label: <none>

Device 2 74.5 GB ref: 16 (Vendor: ATA Model: FUJITSU MH W2080B Rev: 0)
  partition 1 74.5 GB ref: 17 label: 404913186405899C

In this example, the device reference number for the hard disk on the FortiGate-ASM-S08 module is 16 and the partition reference number for the partition on this hard disk is 17. The label 404913186405899C for partition ref 17 indicates that WAN optimization storages have been added to this partition.

Use the following command to add a WAN optimization storage named is_WAN_sto_1 to partition reference number 17. The storage size is 20 GB or 20000 MB.
execute scsi-dev storage 17 20000 WAN_sto_1
Storage created; size: 20000MB signature: WAN-sto_1-
404913186405899C

Example: WAN optimization storage on a FortiGate-111C unit with two hard disks

This example shows how to configure WAN optimization storage on a FortiGate-111C with two hard disks. The example describes how to use the first disk for byte caching and the second disk for web caching. This example does not describe how to install the second hard disk.

To configure WAN optimization storage on a FortiGate-111C with two hard disks

The FortiGate unit finds both hard disks and the single partitions on the hard disks and assigns the disks and partitions reference numbers. Use the following command to display the disk information:

execute scsi-dev list
Device 1 60.2 GB ref: 0 (Vendor: ATA Model: STT_FTM64GL25H Rev: J090)
partition 1 60.2 GB ref: 1 label: 2CC878A743254E58
Device 2 60.2 GB ref: 2 (Vendor: ATA Model: STT_FTM64GL25H Rev: J090)
partition 1 60.2 GB ref: 3 label: 8CC87A746539E28

In the example output, Device 1 is the first hard disk and Device 2 is the second hard disk. The reference number for the first hard disk is 0 and the reference number for the partition on the first hard disk is 1. The reference number for the second hard disk is 2 and the reference number for the partition on the first hard disk is 3. These are example numbers only. They may be different on some units.

Use the following steps to configure the partition on the first disk for byte caching and the partition on the second disk for web caching.

1. Enter the following command to add a WAN optimization storage named byte_cache_sto to be used for byte caching. The command adds the WAN optimization storage to partition reference 1:
   execute scsi-dev storage 1 60000 byte_cache_storage
   Storage created; size: 60000MB signature: byte-cache-sto-
   2CC878A743254E58

   See “About partition labels” on page 122 for more information about adding storages to a partition.

2. Enter the following command to add a WAN optimization storage named web_cache_sto to be used for web caching. The command adds the WAN optimization storage to partition reference 3:
   execute scsi-dev storage 3 60000 web_cache_sto
   Storage created; size: 60000MB signature: web_cache_sto-
   77A2A1A1D0E8F8B7

   See “About partition labels” on page 122 for more information about adding storages to a partition.

   You cannot list these WAN optimization storages using the execute scsi-dev command. Instead, use the following command to list the WAN optimization storages that you have added:
   get wanopt storage
About partition labels

The first time you add a storage to a partition using the `execute scsi-dev storage` command the partition is labelled with a random string (in the example below, `77A2A1AB1D0EF8B7`). This label is used for all storages added to a given partition. A different label is created for each partition. The labels appear when you use the `execute scsi-dev list` command to list the partitions. In the following example, a label is added to partition reference 17.

```sh
execute scsi-dev list
Partition is created on /dev/sdb with file system; size: 40000MB
Device 1 74.5 GB ref: 0 (Vendor: ATA Model: FUJITSU MHW2080B? Rev: 000)
  partition 1 74.5 GB ref: 1 label: <none>
Device 2 60.3 GB ref: 16 (Vendor: IET Model: VIRTUAL-DISK Rev: 0)
  partition 1 39.1 GB ref: 17 label: 77A2A1AB1D0EF8B7
```

3 Enter the following command to configure web caching to use the `web_cache_sto` storage and byte caching to use the `byte_cache_sto` storage:

```sh
config wanopt cache-storage
  set web-cache-storage web_cache_sto
  set byte-cache-storage byte_cache_sto
end
```
Index

A
accept action
firewall policy, 26, 27
accept any peer, 29
active-passive
WAN optimization rules, 37
authentication, 38
authentication method, 33
peer, 30
WAN optimization peer authentication, 29
authentication group
authentication method, 33
certificate, 33
password, 33
pre-shared key, 33

B
bandwidth
maximum, 39
byte cache, 15

C
certificate
authentication group, 33
CIDR, 42
comments, documentation, 13
configuring
WAN optimization peer, 31
customer service, 12

D
default
password, 8
documentation
commenting on, 13
Fortinet, 13

E
explicit mode
WAN optimization, 38, 44
explicit web proxy, 113

F
firewall
policy matching, 40
firewall load balancing, 38
firewall policy, 21, 37
accept action, 26, 27
changing the position in the policy list, 41
deleting, 41
identity-based, 38
insert policy before, 40
matching, 40
maximum bandwidth, 39
moving, 41
traffic priority, 39
FortiClient peer, 22
FortiGate documentation
commenting on, 13
FortiGuard
Antispam, 8
Antivirus, 8
Fortinet customer service, 12
Fortinet documentation, 13
Fortinet Knowledge Center, 13

H
host ID
peer, 22, 29
HTTP
unknown HTTP sessions, 45
HTTP rule
non-HTTP sessions, 45

I
identity-based firewall policies, 38
insert policy before
firewall policy, 40
installation, 8
introduction
Fortinet documentation, 13
IP address
peer, 22
WAN optimization, 29

L
load balancing, 38
local host ID
peer, 29

M
matching
firewall policy, 40
maximum bandwidth, 39
firewall policy, 39
traffic shaping, 39
mode
operation, 8
Index

monitoring
WAN optimization, 25
moving a firewall policy, 41

N
NAT, 38
NAT/Route mode, 22
non-HTTP sessions
HTTP rule, 45

O
operation mode, 8
out of path
topology, 16

P
password
administrator, 8
authentication group, 33
peer
accept any peer, 29
host ID, 22, 29
IP address, 22
local host ID, 29
WAN optimization, 29
peer authentication, 30
WAN optimization, 29
peer host ID
WAN optimization, 29
peer IP address
WAN optimization, 29
peer-to-peer
WAN optimization rules, 37
policy
accept action, 26, 27
changing the position in the policy list, 41
deleting, 41
firewall, 21
insert policy before, 40
matching, 40
maximum bandwidth, 39
move, 41
traffic priority, 39
pre-shared key
authentication group, 33
protocol optimization, 37

R
reverse proxy
web cache, 19, 107
routing
configuring, 113
rule, 37
active-passive, 37
non-HTTP sessions, 45
peer-to-peer, 37
unknown HTTP sessions, 45
WAN optimization, 37

S
secure tunnelling, 15
sharing
WAN optimization tunnels, 23
SSL offloading, 15

T
TCP port
WAN optimization tunnels, 22
technical support, 12
topology
out of path, 16
Traffic Priority, 39
traffic priority
firewall policy, 39
traffic shaping, 39
tunnel
sharing WAN optimization tunnels, 23
TCP port, 22
WAN optimization, 22
tunnel request, 30
tunnel-non-http, 45

U
unknown HTTP sessions, 45

V
VDOMs, 22
virtual domains, 22
virtual IP
WAN optimization, 38

W
WAN optimization
and virtual IPs, 38
explicit mode, 44
FortiGate models supported, 8
IP address, 29
monitoring, 25
peer authentication, 29
peer host ID, 29
peer IP address, 29
peers, 29
transparent mode, 44
WAN optimization peer
configuring, 31
web cache, 15
active-passive WAN optimization, 68
adding to passive WAN optimization rule, 68
client/server WAN optimization, 68
non-standard ports, 66
peer to peer WAN optimization, 72
reverse proxy, 19, 107
Index

web proxy, 113

X

X-Forwarded-For (XFF), 114